

Sicherheitshinweise für Deutsche



„Man kann sich heute nicht in Gesellschaft um Deutschland bemühen; man muß es einsam tun wie ein Mensch, der mit einem Buschmesser im Urwald Bresche schlägt und den nur die Hoffnung erhält, daß irgendwo im Dickicht andere an der gleichen Arbeit sind.“

-Ernst Jünger (Das Abenteuerliche Herz)

Inhaltsverzeichnis

1 Allgemeine Grundsätze und Vordrucke 1

2 Sicherheitshinweise 10
2.1 Angriffe und Bedrohungen durch Linkskriminelle 10
2.2 Schutz durch Aufklärung 10
2.3 Vor einem Angriff 10
2.4 Während eines Angriffes 10
2.5 Nach einem Angriff 11
2.6 Psychologische Aspekte nach einem Angriff 11
2.7 Umgang mit der Polizei 12
2.8 Aussageverweigerung und Verhörmethoden 12
2.9 Die prozessuale Bedeutung der Aussageverweigerung 13
2.10 Warum ist es wichtig, mit einem Anwalt zu sprechen? 14
2.11 Die Aussageverweigerung als Zeuge 14
2.12 Die Aussageverweigerung als Beschuldigter 15
2.13 Die Vernehmungstaktiken 17
2.14 Die Taktik des - Es Ist Das Beste Für Dich 18
2.15 Die Taktik, Kameraden gegeneinander auszuspielen 18
2.16 Die Taktik des - Sie Haben Gewonnen 19
2.17 Psychischer Druck und Entspannung 20
2.18 Aussageverweigerung und Knast/Beugehaft 21
2.19 Falschaussagen 22
2.20 Alibiaussagen 22
2.21 Entlastungszeugen 22
2.22 Erfahrungsbericht: Die Vernehmung 23

3 Datenschutz - Sicherheit 2.0 25
3.1 Datenschutz 26
3.2 Das Passwort 27
3.3 Gefahren für dein Passwort 27
3.4 Passwortwahl 29
3.5 Passwort-Generator 31
3.6 Aufbewahrung von Passwörtern 31
3.7 KeePass Password Safe 33
3.8 Schlüsseldateien - Besser als jedes Passwort 34
3.9 Die Schlüsseldatei 34

4 Datenkraken 35

5 Daten-Striptease 37
5.1 Grundsätzliche Regeln 37
5.2 Schützt eure Daten und Strukturen! 39
5.3 Facebook Sicherheitseinstellungen - Öffentlich vs. Privat 41
5.4 Allgemeine Einstellungen 41
5.5 Privatsphäre-Einstellung 41
5.6 Die richtigen Sicherheitseinstellungen für Twitter 42

6 Tracking verhindern 42
6.1 Flash-Cookies und Super-Cookies löschen lassen 43
6.2 Seitenübergreifende Dienste 43
6.3 Fingerabdruck des Netzbetrachters 44

7 Das Tor-Netzwerk . . . 46
7.1 Funktionsweise von Tor - Was steckt dahinter? . . . 47
7.2 Gefahren des Tor-Netzwerks - Was muss beachtet werden? . . . 48
7.3 Das richtige Paket - Installation und Inbetriebnahme . . . 48
7.4 Tor-Browser richtig einstellen . . . 50
7.5 Spezielle Tor-Browser . . . 52
7.6 Tor-Bad-Exits . . . 52
7.7 Tor-Good-Exits . . . 53
7.8 Tor-Onionland . . . 55
7.9 Kompatibilität verschiedener Weltnetzseiten mit Tor . . . 56
7.10 Das Tor-Netzwerk allein reicht nicht . . . 56
7.11 Weltnetz - Verläufe löschen . . . 56

8 Computer . . . 60
8.1 Betriebssystem - „Tails“ . . . 60
8.2 Dateien löschen - Sind sie wirklich weg? . . . 61
8.3 Grundlagen: Speichern und Löschen von Daten . . . 61
8.4 Wie werden Daten gespeichert . . . 62
8.5 Versteckte Datenspeicher . . . 62
8.6 Daten „zwischen den Zeilen“ . . . 62
8.7 Löschen von Daten . . . 63
8.8 Dateien sicher löschen - durch Überschreiben . . . 63
8.9 Eraser . . . 64
8.10 Datenversand durch Windows verhindern . . . 66
8.11 Die Sache mit den Fotos - Exif-Anhang löschen . . . 66
8.12 JPEG & PNG Stripper . . . 66
8.13 Die virtuelle Maschine . . . 67
8.14 Echtzeitverschlüsselung von Dateien und Datenträgern . . . 68
8.15 Verschlüsselungs- und Hash-Algorithmen von TrueCrypt . . . 68
8.16 Unterstützte Systeme und Installation von TrueCrypt . . . 69
8.17 Deutsche Sprache für TrueCrypt . . . 69
8.18 Erstellen von Datentresoren . . . 70
8.19 Einzelne Festplatte Verschlüsseln . . . 71
8.20 Verschlüsselung der „C:“ Festplatte (Systemfestplatte) . . . 72
8.21 Verschlüsselung der Festplatte mit verstecktem Betriebssystem . . . 74
8.22 TrueCrypt Traveller Disk erstellen . . . 80
8.23 TrueCrypt Volume auf CDs und DVDs . . . 81
8.24 Volume-Optionen von TrueCrypt . . . 81
8.25 Risiken bei Verwendung des Dateisystems NTFS (Host) und der Funktion Defragmentieren . . . 82
8.26 Verwendung von Keyfiles (Schlüsseldateien) . . . 82
8.27 Verwendungsmöglichkeit im Hinblick auf den Bundestrojaner . . . 83
8.28 Hackerschutz („Firewall“) . . . 84
8.29 Firewall und offene Ports . . . 84
8.30 Was eine Firewall bringt - und was nicht . . . 85
8.31 Probleme bei Firewalls . . . 86
8.32 Teste dein System per Portscan . . . 87
8.33 Comodo Firewall . . . 87
8.34 Die Comodo Firewall und OpenVPN . . . 89
8.35 Netzbetrachter („Browser“) . . . 91
8.36 Mozillas Firefox . . . 92
8.37 Wichtige Einstellungen für deinen Firefox . . . 92
8.38 Begrifferklärungen (Browsercheck) . . . 95
8.38.1 ActiveX . . . 96

8.38.2 Cookies . . . 97
8.38.3 Java . . . 98
8.38.4 JavaScript / JScript . . . 98
8.38.5 Phishing . . . 100
8.38.6 Virsual Basic Script . . . 100
8.38.7 XPI-Erweiterungen . . . 101
8.39 Mehr Sicherheit durch Add-Ons . . . 101
8.40 JavaScript blockieren mit NoScript . . . 104
8.41 HTTP Referrer beliebig verändern . . . 105
8.42 HTTPS Everywhere . . . 106
8.43 Adblock Plus - Für ein Web ohne nervige Werbung . . . 106
8.44 Long URL Please . . . 108
8.45 Bloody Vikings . . . 109
8.46 User Agent Switcher . . . 110
8.47 Tracking (Verfolgung durch Webseiten) verhindern . . . 110
8.48 DNS Abfragen verschlüsseln mit DNSCrypt . . . 111
8.49 Firefox Portable . . . 111
8.50 Schutz vor Spionage- und Werbesoftware . . . 112
8.51 Spybot S&D und Ad-Aware . . . 112
8.52 Virenschutz . . . 113
8.53 Computerviren . . . 114
8.54 Trojaner . . . 117
8.55 Hoaxes, Kettenbriefe und falsche Warnungen . . . 118
8.56 Schutz vor Viren, Trojanern und Würmern . . . 119
8.57 Avira AntiVir Personal Free . . . 120
8.58 Weltnetz - Verläufe löschen . . . 121
8.59 Was wird vom cCleaner bereinigt? . . . 121
8.60 WLAN Router - So schützt du dein Funknetz . . . 126
8.61 Gefahren bei WLAN . . . 126
8.62 WLAN-Schutz: Richtig einrichten . . . 127
8.63 Tor-Proxy - Deine Fritz!Box als Tarnkappen-Router . . . 128
8.64 Freeware Freetz: So kommt Tor in die Fritz!Box . . . 128
8.65 Fritz!Box-Firmware konfigurieren . . . 129
8.66 Firmware flashen und Tor einrichten . . . 130
8.67 Tipps für mehr Geschwindigkeit . . . 130
8.68 Weltnetz . . . 131
8.69 Anonymität im Weltnetz . . . 132
8.70 Anonym surfen - Einleitung . . . 132
8.71 Das Ende der Anonymität im Weltnetz? . . . 134
8.72 Sicherheit durch UMTS-Sticks . . . 135
8.73 VPN Server . . . 136
8.74 Methoden zur Verschlüsselung und Anonymisierung . . . 137
8.75 VPN Anbieter . . . 138
8.76 Einrichten der Anonymisierung . . . 139
8.77 Zahlungsmittel besorgen, Registrieren und Bezahlen . . . 139
8.78 Nach Erhalt der Zugangsdaten einrichten des VPN . . . 140
8.79 Einrichten von Proxifier für den Sock5 . . . 142
8.80 DNS an den Proxy anpassen . . . 145
8.81 Mac-Adresse bzw. IMEI (bei UMTS-Sticks) . . . 145
8.82 Der erste Test . . . 145
8.83 DNS Leak . . . 147
8.84 Die digitalen Wolken: Die Cloud Computing Falle? . . . 148
8.85 Sind Daten in einer Cloud sicher? . . . 149
8.86 Anleitung einer sicheren Cloud-Alternative . . . 151

8.87 eBrief Verschlüsselung . . . 152
8.88 Installation von Thunderbird . . . 153
8.89 Einrichtung von Thunderbird . . . 153
8.90 Was ist PGP/GnuPG/OpenPGP? . . . 154
8.91 Was kann GnuPG? . . . 154
8.92 eBrief - Verschlüsselung mit GnuPG . . . 155
8.93 Installation und Vorbereitung . . . 156
8.94 Eigenen öffentlichen Schlüssel versenden . . . 157
8.95 Dateien verschlüsseln und versenden . . . 158
8.96 Dateien entschlüsseln . . . 158
8.97 Sinn und Legitimität der GnuPG-Verschlüsselung . . . 159
8.98 Installation der Erweiterung Enigmail für Thunderbird . . . 159
8.99 Allgemeine Einstellungen von Enigmail . . . 160
8.100 Erzeugen eines Schlüssels . . . 160
8.101 Versenden und Empfangen verschlüsselter eBriefe . . . 161
8.102 Das Problem: Schlüssel Echtheit . . . 161
8.103 Der „Man-in-the-middle“ Angriff . . . 161
8.104 Wie dieser Angriff funktioniert . . . 162
8.105 Schlüssel-Integrität ist der Dreh- und Angelpunkt! . . . 162
8.105.1 Echtheit von Schlüsseln überprüfen . . . 163
8.106 Nachrichtensofortversand . . . 163
8.106.1 Installation von Pidgin . . . 164
8.106.2 Einrichten der Nachrichtenverschlüsselung . . . 165
8.106.3 Beginnen einer sicheren Unterhaltung . . . 165
8.107 Suchmaschine gleich Suchmaschine? . . . 166
8.108 Versand von eBriefen . . . 167
8.108.1 Anonyme eBrief Accounts . . . 168
8.108.2 Private Messages in Foren nutzen . . . 169
8.108.3 Mixmaster-Remailer . . . 169
8.108.4 Spam-Schutz . . . 170
8.108.5 AnonBox des CCC (24-48h) . . . 170
8.108.6 Wegwerf-eBrief-Adressen . . . 170
8.108.7 Temporäre eBrief Adressen . . . 171
8.108.8 eBrief Provider abseits des Mainstream . . . 171
8.109 Vorratsdatenspeicherung und staatliche Überwachung . . . 172
8.109.1 Diese Daten wurden gespeichert . . . 172
8.109.2 Wer speichert die Verbindungsdaten - und wie lange? . . . 173
8.109.3 Welche Bestandsdaten werden gespeichert? . . . 173
8.109.4 Ist das letzte Wort schon gesprochen? . . . 174

9 Mobiltelefon . . . 174
9.1 Demotipps für den sicheren Umgang mit Mobiltelefonen . . . 175
9.2 Vor der Demo . . . 175
9.3 Auf der Demo . . . 176
9.4 Hilfe, ich werde verhaftet . . . 177
9.5 Nützliche Informationen zu deinem Mobiltelefon . . . 177
9.6 Wie funktioniert das Mobiltelefon? . . . 178
9.7 Die stille SMS . . . 179
9.8 Der IMSI - Catcher . . . 180
9.9 Was heisst das? Ein Beispiel 181
9.10 Zusammenfassung . . . 182
9.11 Smartphone Sicherheit . . . 183
9.12 Sicherheitslücken von Smartphones stopfen . . . 183
9.13 Android Berechtigungen - Alles oder nichts . . . 186

9.14 Wichtige APPs für dein Smartphone . . . 190
9.15 Antivirus . . . 190
9.16 APG . . . 194
9.17 App Guard . . . 195
9.18 ChatSecure . . . 198
9.19 DuckDuckGo . . . 199
9.20 Ich bekomme Arrested . . . 199
9.21 K-9 Mail . . . 200
9.22 KeePassDroid . . . 201
9.23 Mozilla Firefox . . . 202
9.24 https Everywhere - Add-On . . . 202
9.25 No Script - Add-On . . . 202
9.26 Proxy Mobile - Add-On . . . 203
9.27 Ghostery - Add-On . . . 203
9.27.1 Note Cipher . . . 203
9.28 ObscuraCam . . . 204
9.29 OpenVPN . . . 204
9.30 Orbot & Orfox . . . 204
9.31 Passwort-Generator . . . 205
9.32 Signal und Conversations - „Sichere“ Messenger . . . 206
9.33 Verschlüssel dein Android-Smartphone . . . 207
9.34 Sicherheitsrisiko für Mobiltelefone: Öffentliche Ladestationen . . . 209
9.35 Root?! . . . 209

10 Selbstverteidigung . . . 211
10.1 CS-Gas . . . 212
10.2 Elektroschocker . . . 213
10.3 Schreckschuss- Gaspistolen . . . 214
10.4 Jet Protector . . . 215
10.4.1 Kubotan / Tacticalpen . . . 216
10.4.2 Pfefferspray . . . 216
10.5 Schlagstock . . . 217
10.6 Schrillalarm . . . 217
10.7 Selbstverteidigungsschirm . . . 218
10.8 Taktische Taschenlampe . . . 219

11 Rechtsratgeber . . . 219
11.1 Rechte im Umgang mit der Polizei in Brandenburg . . . 219
11.1.2 Befragung - was musst Du sagen ? . . . 220
11.1.3 Durchsuchung von Personen und Sachen . . . 221
11.1.4 Verhältnismäßigkeit . . . 223
11.1.5 Nachwort . . . 223
11.2 Verfassungsschutz - Anquatschversuche . . . 223
11.2.1 Von wem wirst Du angequasselt? . . . 225
11.2.2 Warum wirst gerade DU angequasselt? . . . 226
11.2.3 Was tun, wenn du angequasselt wirst? . . . 226
11.2.4 Anwerbeversuche sofort bekannt machen! . . . 228
11.2.5 Dein Gedächtnisprotokoll . . . 228
11.2.6 Welchen Schaden richten Spitzel an? . . . 229
11.2.7 Wie können wir uns schützen? . . . 230
11.2.8 Wenn Spitzel fliegen lernen... . . . 231
11.2.9 Die einzige Konsequenz: Null Toleranz! . . . 232
11.3 Verhalten bei Demonstrationen . . . 232

11.4 Verhalten bei einem feindlichen Outing . . . 233
11.4.1 Die Vermischung legaler und illegaler Methoden . . . 234
11.4.2 Dein Recht auf Aussageverweigerung . . . 235
11.4.3 Warum ist es wichtig, mit einem Anwalt zu sprechen . . . 236
11.4.4 Die prozessuale Bedeutung der Aussageverweigerung . . . 236
11.4.5 Die Spekulation mit deiner Angst . . . 236
11.4.6 Hausdurchsuchungen . . . 237
11.4.7 Erfahrungsprotokoll - Eine Hausdurchsuchung . . . 238
11.4.8 Festnahmen . . . 239
11.4.9 Erkennungsdienstliche Maßnahmen . . . 240
11.4.10 Die Einschüchterungstaktiken . . . 240
11.4.11 Erfahrungsbericht: Allein auf dem Revier . . . 241
11.4.12 Wovor haben die Polizeibeamten und die Herrschenden Angst ? . . . 242
11.4.13 Deine Schwäche ist Deine Stärke . . . 242
11.4.14 Die Vernehmungstaktiken . . . 242
11.4.15 Die Taktik des „Es ist das beste für Dich“ . . . 243
11.4.16 Gespräche von „Mensch zu Mensch“ . . . 244
11.4.17 Erfahrungsbericht: Die Vernehmung . . . 245
11.4.18 Die Taktik des „Sie haben gewonnen“ . . . 247
11.4.19 Die Taktik, Kameraden gegeneinander auszuspielen . . . 247
11.4.20 Wie bekommst Du Kontakt zur Außenwelt ? . . . 248
11.4.21 Untersuchungshaft . . . 249
11.4.22 Erfahrungsbericht: In der Zelle . . . 249
11.4.23 Den Knast studieren . . . 251
11.4.24 Dein Verhalten gegenüber den Beamten . . . 252
11.4.25 Welcher Anwalt ? . . . 254
11.4.26 Kosten für den Anwalt . . . 254
11.4.27 Prozesskostenbeihilfe . . . 255
11.4.28 Dein Verhalten gegenüber Polizei und Justiz - Zusatzblatt . . . 255
11.4.29 Polizeikonzepte aufdecken! . . . 256
11.4.30 Ein Rahmenkonzept zur Bekämpfung der Rockerkriminalität . . . 257
11.5 Wir bilden Bezugsgruppen . . . 260
11.5.1 Warum eine Bezugsgruppe? . . . 261
11.5.2 Was ist eine Bezugsgruppe? . . . 262
11.5.3 Grundlagen . . . 262
11.5.4 Fragerunde . . . 263
11.5.5 Rollenverteilung . . . 264
11.5.6 Vorbereitung auf Aktion . . . 267
11.5.7 Aktionsformen (Beispiele) . . . 268
11.5.8 Übung macht den Meister . . . 273
11.5.9 Nach der Aktion . . . 273
11.5.10 Schlusswort . . . 274

12 Allgemeine Hinweise . . . 275
12.1 Anti-Antifa - Kleines Einmaleins für die Recherche . . . 275
12.1.1 Recherche als Grundlage politischer Arbeit . . . 275
12.1.2 Recherche gegen Linkskriminelle . . . 276
12.1.3 Quellen der Recherche . . . 277
12.2 Selbstverständlich Wahlbeobachter - Aber wie? . . . 279
12.2.1 Vorbereitung der Wahlbeobachtung . . . 280
12.2.2 Beobachtung der „Auszählung“ . . . 281
12.2.3 Probleme? . . . 281
12.2.4 Nach der Wahl . . . 282

12.3 Wie erstellt man ein Flugblatt? . . . 282
12.3.1 Gestaltung eines Flugblattes - A I D A . . . 282
12.3.2 Wichtig: V.i.S.d.P. . . . 283
12.3.3 Drucken eines Flugblattes . . . 283
12.3.4 Verteilen eines Flugblattes . . . 285
12.4 Wie erstellt man ein Transparent? . . . 285
12.4.1 Erfolgsrezepte und Todsünden . . . 285
12.4.2 Das regenfeste und sehr haltbare Bilder-Transparent . . . 286
12.4.3 Das klassische Bettlaken-Transparent . . . 287
12.4.4 Schablonentechnik . . . 289
12.4.5 Bilder und Symbole auf Transparenten . . . 290
12.5 Wie erstellt man eine Sprühschablone? . . . 291
12.5.1 Was wird benötigt? . . . 291
12.5.2 Motiv zeichnen und ausschneiden . . . 292
12.5.3 Falls die Schablone instabil ist . . . 292
12.5.4 Kreative Anwandlung . . . 292
12.6 Wie erstellt man einen Spuckie? . . . 293
12.6.1 Was wird benötigt? . . . 293
12.6.2 Wo kriegst du einseitig vorgummiertes Papier her? . . . 293
12.6.3 Erstellen der Vorlage . . . 293
12.6.4 Ausdrucken der Vorlage: . . . 294
12.6.5 Das Ausschneiden der Spuckies . . . 294
12.7 Wie erstellt man Wurfschnipsel . . . 295
12.7.1 Was wird benötigt? . . . 295
12.7.2 Erstellen des Wurfschnipsels . . . 295
12.7.3 Nach der Aktion . . . 295
12.8 Wie erstellt man eine sichere Weltnetzseite? . . . 295
12.8.1 Anonyme Weltnetzseite, Webserver, Domains und Hosting . . . 296
12.8.2 Gefahren und Sperren von Domain und oder Webserver . . . 297
12.8.3 Domain ¡=¿ DNS ¡=¿ Webserver - Wie geht man damit um? . . . 298
12.8.4 Kommen wir nun zu einer ernsthaften Weltnetzseite . . . 299
12.8.5 Eine Weltnetzseite mit WordPress auf einem Webspace erstellen . . . 301
12.9 Anmelden einer Demo und Umgang mit den Behörden . . . 306
12.9.1 Anmeldung einer Versammlung . . . 306
12.9.2 Spontanversammlungen . . . 306
12.9.3 Sofortversammlungen . . . 307
12.9.4 Eilversammlungen . . . 307

1 Allgemeine Grundsätze und Vordrucke

Eine gute Sicherheitskultur ist mit eine der wirksamsten Waffen die wir haben. Unsere Gegner haben ihre Spione,Spitzel und Informanten überall. Haltet alle Gruppen klein und vertraulich. Eine Person ist für viele Sachen genug - die Anzahl drei sollte nicht überschritten werden. für sehr große Aktionen kommen mehrere dreier Gruppen zusammen. In so großen Gruppen solltet ihr aber keine grauen Sachen machen. Bezugsgruppen sollten nur aus Leuten bestehen die sich schon Jahre kennen. Das verringert das Risiko der Infiltration. Trotzdem: vertraut niemandem - nehmt das ernst! Es ist niemandem geholfen, wenn ihr für nichts in den Bau wandert. Punkte an die ihr euch halten solltet, als würde euer Leben davon abhängen:

- GIB NIEMALS mit durchgeführten Aktionen an!
- BENUTZT NIEMALS KLARNAMEN wenn ihr eine Aktion plant - nutzt Fantasienamen!
- Bespreche Aktionen nur mit denen die etwas wissen müssen!
- Nach Aktionen: NIEMALS MIT Außenseitern BESPRECHEN!
- GIB NIEMALS ETWAS ZU! Selbst wenn sie dir einen Deal vorschlagen und behaupten sie wüssten Bescheid weil andere gesungen haben. Wenn du noch nicht gesungen hast, haben die anderen es höchstwahrscheinlich auch noch nicht getan!
- SAG DEN Staatsdienern NIEMALS IRGENDETWAS - SCHWEIGE!
- Denke nicht, dass der Freund eines Freundes ein Freund ist!
- Gehe davon aus, dass JEDER ein Bulle ist und sei entprechend zurückhaltend.
- Gehe davon aus, dass JEDES Telefon abgehört wird - Gespräche können auch mit abgeschaltetem Telefon mitgehört werden. Das gleiche gilt für Laptops, Fernsehr etc.!
- Halte die Anzahl der Leute bei einer Aktion sehr klein.
- Arbeite nur mit Leuten, denen du traust.
- Sprich nur über Aktionen an offenen Orten wie Wald oder Parks.
- Sprich niemals über Aktionen in ÖFFENTLICHEN VERKEHRSMITTELN, dem Auto, Zuhause, öffentlichen Treffplätzen etc.
- Wenn du gefasst wirst, mach von deinem SCHWEIGERECHT gebrauch!
- Verpfeiffe NIEMALS einen anderen Aktivist!
- Sei besonders vorsichtig bei Partnern in Beziehungen (sexuell und romantisch) - Sag besser nichts.
- VERTRAUE NIEMALS komplett auf elektronische VERSCHLÜSSELUNG oder anderen CODEWÖRTERN um deine Kommunikation geheim zu halten! Verschlüsselung dient dazu die Gegner zu verlangsamen! Überwachung = Unterdrückung.
- ÜBERPRÜFE regelmäßig deine Brieftasche und deine Wohnung auf belastendes Material (entfernen oder woanders lagern).
- Vermeide unnörige Kriminaltität wie z.B. Ladendiebstahl, Alkohol am Steuer etc. - dies führt sehr oft zu Folgeuntersuchungen.
- Denkt daran: nur weil wir nicht gewalttätig sind, heißt das noch lange nicht, dass wir nicht als Bedrohung empfunden werden und wir entsprechend behandelt werden.

Auf den folgenden Seiten findet ihr Vordrucke, die euch helfen können:

Hans Mutig
Neue Straße 1
12345 Oberstadt

An die
Staatsanwaltschaft bei dem
Landgericht Oberstadt
Hauptstr. 1
12000 Oberstadt

Sehr geehrte Damen und Herren !

Hiermit erstatte ich Strafanzeige

gegen

1) den Staatsanwalt
2) die fünf Polizisten, die am 02.05.1995 bei mir Hausdurchsuchung hielten, wegen Hausfriedensbruch und Diebstahls.

Außerdem stelle ich hiermit Strafantrag.

Begründung:

Am 02.05.1995 fand bei mir eine Hausdurchsuchung statt. Ich füge den Hausdurchsuchungsbefehl des Amtsgerichtes Oberstadt vom.., Aktenzeichen... bei. Daraus ergibt sich, dass die Hausdurchsuchung gegen mich wegen eines Strafverfahrens wegen unerlaubten Waffenbesitzes und zur Auffindung einer Schusswaffe durchgeführt wurde.
Eine Waffe wurde bei mir aber nicht gefunden, wie sich aus dem Durchsuchungsprotokoll ergibt, dass ich in Kopie beifüge.

Die Polizisten haben vielmehr entgegen § 108 StPO systematisch nach Zufallsfunden gesucht und die beschlagnahmten 10 Bücher "Grimms Märchen" nicht zufällig gefunden. Die Beamten haben 4 Stunden lang Hausdurchsuchung gehalten. Außerdem handelt es sich bei den Büchern um keine Schusswaffe, die Bücher haben mit der Waffe auch nichts zu tun. (KG Strafverteidiger 1985, 404).

Dadurch, dass die Beamten gegen meinen Willen 4 Stunden lang nicht nach einer Schusswaffe suchten, sondern systematisch nach anderen Gegenständen, haben sie einen Hausfriedensbruch begangen.

Als Zeugen benenne ich Max Müller, ...

Bitte teilen Sie mir das Ende des Strafverfahrens mit.

Mit freundlichem Gruß

Hans Mutig (eigenhändige Unterschrift)

Hans Mutig
Neue Straße 1
12345 Oberstadt

An das
Polizeipräsidium Oberstadt
Niederstr. 1
12000 Oberstadt

Sehr geehrte Damen und Herren !

Hiermit erhebe ich gegen die Polizeibeamten, die am 02.05.1995 bei mir eine Hausdurchsuchung durchgeführt haben, Dienstaufsichtsbeschwerde.

Begründung:

Am 02.05.1995 fand bei mir eine Hausdurchsuchung statt. Ich füge den Hausdurchsuchungsbefehl des Amtsgerichtes Oberstadt vom..., Aktenzeichen... bei. Daraus ergibt sich, dass die Hausdurchsuchung gegen mich wegen eines Strafverfahrens wegen unerlaubten Waffenbesitzes und zur Auffindung einer Schusswaffe durchgeführt wurde.

Eine Waffe wurde bei mir aber nicht gefunden, wie sich aus dem Durchsuchungsprotokoll ergibt, dass ich in Kopie beifüge.

Die Polizeibeamten haben bei mir zu Beginn der Hausdurchsuchung nicht ihre Dienstausweise vorgelegt, obwohl ich sie mehrfach darum ersucht hatte. Ich wies darauf hin, dass es heutzutage Kriminelle gibt, die sich als Polizisten, Gasmänner usw. ausgeben, und dass ich die Beamten nicht persönlich kenne. Sie zeigten mir dennoch ihre Ausweise nicht und betraten dann ohne weiteres die Wohnung.

Beweis: Zeugnis Max Müller,...

Außerdem haben die Polizisten entgegen § 108 StPO systematisch nach Zufallsfunden gesucht und die 10 beschlagnahmen Bände "Grimms Märchen" nicht zufällig gefunden. Sie hätten nur nach der Schusswaffe suchen dürfen. Bei den Büchern handelte es sich aber nicht um eine Schusswaffe. Außerdem haben die Beamten 4 Stunden lang meine Wohnung durchsucht, so dass auch dieser Umstand gegen eine zufällige Auffindung der Bücher spricht.

Beweis: Zeugnis Max Müller,...

Die Beschlagnahme der Bücher war rechtswidrig, und es besteht hieran ein Beweisverwertungsverbot (KG Strafverteidiger 1985, 404).

Bitte teilen Sie mir das Ergebnis Ihres Verfahrens mit.

Mit freundlichem Gruß

Hans Mutig (eigenhändige Unterschrift)

Hans Mutig
Neue Straße 1
12345 Oberstadt

An das
Amtsgericht Oberstadt
Am Markt 1
1200 Oberstadt

Sehr geehrte Damen und Herren !

Hiermit lege ich gegen Ihren Hausdurchsuchungsbefehl vom..., Aktenzeichen..., Beschwerde ein und beantrage, mir die bei der Hausdurchsuchung beschlagnahmten 10 Bände "Grimms Märchen" sofort herauszugeben.

Begründung:

Am 02.06.1995 fand bei mir eine Hausdurchsuchung statt. Ich füge Ihren Hausdurchsuchungsbefehl vom... bei. Dabei wurden 10 genannten Bücher beschlagnahmt.

Meine Beschwerde ist jetzt noch zulässig, weil eine Wiederholungsgefahr besteht. Bei mir wurden im letzten Jahr fünf Hausdurchsuchungen durchgeführt. Ich füge die fünf Hausdurchsuchungsbefehle dieser Maßnahmen in Kopie bei. Es steht zu vermuten, dass auch in Zukunft weitere Hausdurchsuchungen gegen mich stattfinden werden.

Meine Beschwerde ist auch begründet. Der Hausdurchsuchungsbefehl ist ungenau. Er enthält nur den ungenauen Satz, dass ein Strafverfahren wegen Volksverhetzung gegen mich eingeleitet sei, und dass die Durchsuchung "zur Auffindung von Beweismitteln führen" werde. In dem Hausdurchsuchungsbefehl fehlt die Angabe des Grundes, warum ich der Volksverhetzung beschuldigt werde. Was soll ich getan haben? Außerdem fehlt in dem Hausdurchsuchungsbefehl die Angabe, nach welchen Beweismitteln gesucht wurde. Werden Bücher gesucht oder Flugblätter? Welchen Titel sollen sie haben? Der Hausdurchsuchungsbefehl ist daher rechtswidrig (BVerfGE 42, 212 und BVerfGE 44, 353 und BVerfG NJW 1992, 551).

Die Beschlagnahme der 10 Bücher aufgrund des rechtswidrigen Hausdurchsuchungsbefehls ist damit auch rechtswidrig. Es besteht an den Büchern ein Beweisverwertungsverbot. Die Bücher sind daher sofort an mich herauszugeben (Krekeler, NStZ 1993, 263, 265).

Mit freundlichem Gruß

Hans Mutig (eigenhändige Unterschrift)

Max Mustermann

Musterstraße 5

12345 Musterstadt

Amtsgericht Musterstadt

Strafabteilung

Willkürstraße 12

12345 Musterstadt

12.08.2012

In der Strafsache gegen meine Person

Aktenzeichen der Durchsuchung und Aktenzeichen der vorgeworfenen Straftat

Hiermit beantrage ich die gerichtliche Entscheidung gemäß § 98 Abs. 2 StPO wegen der Beschlagnahme

folgender Gegenstände, die sich in meinem Besitz befanden:

ein Flyer "Keine Macht der Finanzwirtschaft - www.infoportal-schwaben.net"

ein Klapphandy, grau

ein dazugehöriges Ladegerät

neun Fackeln

ein Laptop, Toshiba

ein dazugehöriges Netzteil

die dazugehörige graue Laptoptasche

ein Karton (Deutsche Post) mit Flugblättern

ein Karton, der weiße Handschuhe und Flugblätter enthält

eine Schachtel (Vodafone), Inhalt: diverse Aufkleber

ein Flugblatt, Thema: "Dresden"

ein Aufnäher aus Stoff "Gegen Repression"

Begründung:

Bei mir fanden am 18. Juli 2012 an meinem Wohnsitz in der Musterstr.5, sowie in der Schwabenstraße 6 an meinem Arbeitsplatz in 12345 Musterstadt und 12354 Musterdorf ab 8.20 Uhr Durchsuchungen statt. Dabei wurden die genannten Gegenstände sichergestellt. Es ist offenkundig, dass diese Gegenstände nicht geeignet sind, mir nachzuweisen, [welche Straftat auch immer] begangen zu haben. Auch für eine andere Straftat ergibt sich aus ihnen kein Anfangsverdacht.
Von der Festplatte des Computers und den Speichern der Mobiltelefone sind – soweit die darauf befindlichen Daten für die Ermittlungen als erforderlich erachtet werden – Kopien zu fertigen. Computer und Telefon selbst sind umgehend an mich herauszugeben (vgl. BVerfG Beschluss vom 12.04.2005, Az. 13 BvR 1027/02, NJW 2005, 1917; BVerfG Urteil vom 02.03.2006, Az. BvR 2099/04, NJW 2006, 976).

Unterschrift

Anlage: Kopie des Durchsuchungsprotokolls

Sicherheitshinweise für Nationalisten



Unzählige gerichtliche Verfahren wurden Verloren weil die davon betroffenen Aktivisten nicht auf ihre Sicherheit, insbesondere auf die Computersicherheit geachtet haben und was noch viel Schlimmer ist, sie auf die miesen Tricks der Polizei reingefallen sind.
Solche Verurteilungen müssen verhindert werden und mit einer konsequenten Einstellung gegenüber den Staatsbütteln und der Verschlüsselung des eigenen Computers, hätte es das ein oder andere mal auch ganz anders ausgehen können.

Auf der SfN Weltnetzseite findest du den theoretischen Teil dieses Selbstschutzes.
Es liegt an dir selbst was du für dich und deine Sicherheit übernimmst. Wir bieten für Jung und Alt eine gute Möglichkeit das hoffentlich schon vorhandene Grundwissen noch einmal auffrischen zu können. Gerade für die Jungen, oftmals unerfahrenen Aktivisten, wollen wir eine wichtige Bezugsquelle sein um sich über die Themengebiete zu informieren.

- Aussageverweigerung und Verhörmethoden
- Datenschutz - Moderne Technik
- Verfassungsschutz - Anquatschversuche
- Verhalten bei Demonstrationen
- Verhalten bei einem feindlichen "Outing"
- Verhalten bei einer Hausdurchsuchung
- Verhalten gegenüber Polizei und Justiz

Schütze dich und dein Umfeld indem du die Theorie beherzigst und sie in die Praxis umwandelst.



www.s=f=n.org

V.i.S.d.P.: S.Richter - Seestr. 5 - 13353 Berlin

Sicherheitshinweise für Nationalisten



Unzählige gerichtliche Verfahren wurden Verloren weil die davon betroffenen Aktivisten nicht auf ihre Sicherheit, insbesondere auf die Computersicherheit geachtet haben und was noch viel Schlimmer ist, sie auf die miesen Tricks der Polizei reingefallen sind.
Solche Verurteilungen müssen verhindert werden und mit einer konsequenten Einstellung gegenüber den Staatsbütteln und der Verschlüsselung des eigenen Computers, hätte es das ein oder andere mal auch ganz anders ausgehen können.

Auf der SfN Weltnetzseite findest du den theoretischen Teil dieses Selbstschutzes.
Es liegt an dir selbst was du für dich und deine Sicherheit übernimmst. Wir bieten für Jung und Alt eine gute Möglichkeit das hoffentlich schon vorhandene Grundwissen noch einmal auffrischen zu können. Gerade für die Jungen, oftmals unerfahrenen Aktivisten, wollen wir eine wichtige Bezugsquelle sein um sich über die Themengebiete zu informieren.

- Aussageverweigerung und Verhörmethoden
- Datenschutz - Moderne Technik
- Verfassungsschutz - Anquatschversuche
- Verhalten bei Demonstrationen
- Verhalten bei einem feindlichen "Outing"
- Verhalten bei einer Hausdurchsuchung
- Verhalten gegenüber Polizei und Justiz

Schütze dich und dein Umfeld indem du die Theorie beherzigst und sie in die Praxis umwandelst.

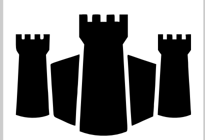


www.s=f=n.org

V.i.S.d.P.: S.Richter - Seestr. 5 - 13353 Berlin

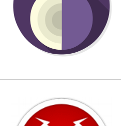
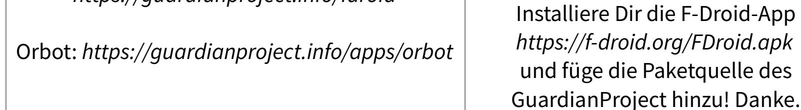
SCHUTZ VOR ÜBERWACHUNG UND BESPITZELUNG

Nutzen! Herunterladen! Verbreiten!
Ausreden zählen nicht,
es geht um Dein Überleben!
https://logr.org/selbstschutz/schutzschild

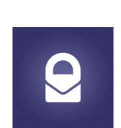


Keine Telefone bei Demos & Aktionen!
Polizei und Behörden hören ab
und spionieren Teilnehmer aus!
https://www.kuketz-blog.de/?s=IMSI-Catcher

ANWENDUNGEN FÜR DEIN „SCHLAUES" TELEFON

  	 **Signal / LibreSignal (Google-Frei)** (auch genutzt von Edward Snowden) Installation: *https://www.whispersystems.org* Kritik: *https://www.kuketz-blog.de/?s=Signal* - BESSERE ALTERNATIVE -  **Conversations** *https://f-droid.org/app/eu.siacs.conversations*	Abhörsichere Kommunikation (verschlüsselte Anrufe und Text) für Android und Apple iPhone. Benötigt Internetverbindung. **Sehr wichtige Pflichtanwendung!** **WhatsApp wird überwacht! Lesen:** **https://logr.org/selbstschutz/whatsapp** Anleitung: *https://www.kuketz-blog.de/conversations-sicherer*
 	**Silence** *https://silence.im* Herunterladen über die F-Droid-Anwendung *https://f-droid.org/app/org.smssecure.smssecure*	Verschlüsselte SMS für Androiden. Benötigt keine Internetverbindung. Unbedingt bei Telefontarifen ohne gebuchtem Internet verwenden!
  	**Orfox und Orbot** Orfox: *https://guardianproject.info/apps/orfox* **Paketquelle des GuardianProject** *https://guardianproject.info/fdroid*  Orbot: *https://guardianproject.info/apps/orbot*	Komplette Anonymisierung aller Internetverbindungen Deines Android-Telefons. Benötigt ROOT. (siehe *www.xda-developers.com/root*) Installiere Dir die F-Droid-App *https://f-droid.org/FDroid.apk* und füge die Paketquelle des GuardianProject hinzu! Danke.
 	 **Android IMSI-Catcher Detector** Weltnetzseite: *https://git.io/AIMSICD* Presseberichte: *https://git.io/vrggR* - ALTERNATIVE - **SnoopSnitch** *https://f-droid.org/app/de.srlabs.snoopsnitch*	App eines Patrioten. Warnt Nutzer bei Angriffen auf die Mobilfunkverbindung durch gefälschte Mobilfunkstationen. **Status: ALPHA. Entwickler gesucht!** Nicht für alle Telefone. Benötigt ROOT. (siehe *www.xda-developers.com/root*)

ANWENDUNGEN FÜR DEINEN RECHNER

 	**Tor Browser** (auch genutzt von Edward Snowden) *https://www.torproject.org* **Betriebssystem inklusive Tor für Aktivisten** *https://tails.boum.org/index.de.html*	Weltnetzbetrachter für die anonyme Internetnutzung. Ersetze damit Deinen Firefox / Internet Explorer / Opera und alle anderen unsicheren „Browser"!  **Sehr wichtige Pflichtanwendung!**
 	**VeraCrypt** *https://veracrypt.codeplex.com* **Videoanleitungen** *https://logr.org/selbstschutz/datentresor*	Verschlüsselung von Speichermedien wie USB-Stifte und Festplatten gegen „Beweise" bei Hausdurchsuchungen. Verbesserter TrueCrypt-Nachfolger. **Sehr wichtige Pflichtanwendung!**
 	**ProtonMail** *https://protonmail.com* Android: *https://goo.gl/7ODFbW* iPhone und iPad: *https://appsto.re/i67D32v*	Sehr sicherer E-Post-Anbieter mit Ende-zu-Ende-Verschlüsselung von unseren guten alten Schweizern. Ersetze damit Dein altes E-Post-Konto! **Sehr wichtige Pflichtanwendung!**

Weitere quelloffene Anwendungen zum Schutz vor dem Überwachungswahn findest Du unter *https://prism-break.org/de*
Sicherheitshinweise im Umgang mit Hausdurchsuchungen, Spitzeln und Festnahmen: *https://s-f-n.org*

V.i.S.d.P.: **Thor**sten **Hammer**, Sonnenweg 88, 12101 Tempelhof (kein Posteingang) • **Version 2.0** • Zur Sicherheit ohne Metadaten: *https://logr.org/selbstschutz/metadaten*



Immigration als Waffe - Jährlich 1,5 Millionen Einwanderer aus der Dritten Welt sollen Europas Intelligenz senken

Rassismus ist das Standardargument schlechthin, wenn Kritiker einer unkontrollierten Zuwanderungspolitik mundtot gemacht werden sollen. Ein Blick in die Geschichte zeigt jedoch, dass erstaunlicherweise gerade einflussreiche Befürworter einer multikulturellen Gesellschaft oftmals mit Biologismus argumentiert haben.

Mit Blick auf den europäischen Kontinent hatte **Richard Nicolaus Graf von Coudenhove-Kalergi** etwa im Jahr 1925 in seiner Programmschrift "Praktischer Idealismus" die **Entstehung einer "eurasisch-negroiden Zukunftsrasse"** vorausgesagt. Äußerlich der altägyptischen ähnlich, sollte diese Mischrasse nach Meinung des Gründers der Paneuropa-Union, die "Vielfalt der Völker durch eine Vielfalt der Persönlichkeiten" ersetzen. Bis heute sehr aufschlussreich sind die Ansichten Coudenhove-Kalergis zu den **Juden**, die er als die "geistige Führerrasse Europas" bezeichnete. In der Öffentlichkeit weit weniger bekannt sind die Gedanken des US-amerikanischen **Juden** und Anthropologen **Earnest Hooton**, der die Deutschen unterschiedslos für "moralische Schwachsinnige" hielt. In einem 1943 veröffentlichten Aufsatz hatte Hooton empfohlen, **die Geburtenzahl der Deutschen zu reduzieren sowie die Einwanderung und Ansiedlung von Nicht-Deutschen, insbesondere von Männern, in Deutschland zu fördern.** Um größeren Widerstand bei den Deutschen zu vermeiden, schlug Hooton vor, diese "Umzüchtung" langsam durchzuführen.

Dass Ideen einer gezielten Völkervermischung bis heute ihre Anhänger haben, macht das Beispiel des 1962 in Chilton, Wisconsin, geborenen US-amerikanischen Forschers auf dem Gebiet der Militärstrategie **Thomas Barnett** deutlich. In Büchern wie "The Pentagons New Map" und "Blueprint for Action" nennt der als "Vordenker der Globalisierung" bezeichnete Barnett als Endziel der US-Politik die **"Gleichschaltung aller Länder der Erde".** Gerade vor dem Hintergrund der aktuellen Immigrationswelle interessant sind Barnetts Gedanken zu Europa. **Der Kontinent soll nach Ansicht des Geostrategen jährlich 1,5 Millionen Einwanderer aus der Dritten Welt aufnehmen.** Ähnlich wie bei Coudenhove-Kalergi taucht der Gedanke auf, dass in Europa die Entstehung einer "hellbraunen Rasse" gezielt herbeigeführt werden müsste. **Ergebnis wäre laut Barnett eine Bevölkerung mit einem durchschnittlichen Intelligenzquotienten von 90, "zu dumm zu begreifen, aber intelligent genug, um zu arbeiten".**

YouTube.com: Sarkozy Hooton (Bestätigung durch den französischen Präsidenten)
Hilf mit, das zu verhindern unter: **einprozent.de** und **deraustausch.at**
www.startpage.com: **"Handbuch zum Selbsterhalt".pdf (Was du tun kannst)**

-BITTE VERBREITEN-

2 Sicherheitshinweise

2.1 Angriffe und Bedrohungen durch Linkskriminelle

Angriffe und Bedrohungen durch Linkskriminelle sich leider keine Seltenheit. Gerade in größeren Städten wie Berlin gehören sie fast zum Alltag.

Grundsätzlich muss jeder politische Aktivist aus unseren Reihen davon ausgehen, dass er zu einem x-beliebigen Zeitpunkt Opfer eines linkskriminellen „Hausbesuches“ bzw. Anschlages wird. Dies betrifft keineswegs nur öffentlich bekannte Aktivisten, wenngleich solche wesentlich stärker gefährdet sind. Niemand von uns kann wissen, was andere über uns wissen.

2.2 Schutz durch Aufklärung

Das Risiko von Überfällen und Anschlägen kann deutlich vermindert werden, wenn man seine Pappenheimer kennt. Schau dich in deiner näheren und auch in der weiteren Umgebung um, wo potentielle linke Täter und deren Treffpunkte zu finden sein könnten. Finde Namen und Adressen heraus und lass sie wissen, dass sie dir bekannt sind. Wenn linkskriminelle Täter nicht mehr aus der Anonymität heraus agieren können und selbst etwas zu verlieren haben, dann vergeht vielen die Lust auf Kleinkriege vor der eigenen Haustür.

Das ist natürlich keine Garantie, aber zumindest ist ihnen dann bewusst, dass sie als erste die Konsequenzen zu spühren bekommen könnten, wenn dir etwas zustoßen sollte. Eine konsequente Anti-Antifa-Arbeit ist deshalb unerlässlich.

2.3 Vor einem Angriff

Es ist natürlich auch immer sinnvoll Angebote zu nutzen die kenntnisse über Selbstverteidigungstechnicken vermitteln.
Waffen wie Teleskopschlagstöcke oder Gaspistolen geben dir sicher ein Gefühl von Sicherheit, dennoch raten wir dir ab diese mitzuführen da sie im Ernstfall:

ein zusätzliches Risiko auch für dich werden können das Tragen dieser Waffen in der BRD nur mit entsprechender Genehmigung gestattet ist und Zuwiderhandlungen hart bestraft werden können.

Wir empfehlen daher die Verwendung von Gas-Sprays wie z.B. CS-Gas oder Pfefferspray. Natürlich musst du auch bei diesen Waffen aufpassen wann und wo du diese einsetzt aber solange du sie nicht in geschlossenen Räumen oder bei Gegenwind einsetzt bist du meistens aus der Gefahrenzone. Weiterhin Hilfreich sind akustische Geräte, die einen ohrenbetäubenden Lärm produzieren und Passanten alarmieren.
Zum Auftreten in der Öffentlichkeit gibt es auch einige Hinweise: Linkskriminelle suchen sich ihre Opfer nicht willkürlich aus. Natürlich wollen sie nicht, dass das Opfer sich eventuell wehren könnte oder ihnen gar körperlich übelegen ist.
Gefragt ist also eine Ausstrahlung die anderen mitteilt:
NICHT MIT MIR !!
Es ist wichtig Blickkontakt mit dem potenziellen Angreifer zu halten. Versuche ihn einzuschätzen und seinen nächsten Schritt voraus zu berechnen.
Sei in jedem Fall vorbereitet - das nützt dir in verschiedener Hinsicht. Du versteinerst nicht vor Schreck und kannst dich auf einen möglichen Angriff einstellen.

2.4 Während eines Angriffes

Je nach Art des Angriffes kann kluges Verhalten unterschiedlich aussehen. Du solltest auf jeden fall Ruhe bewahren. Vermeide Handlungen wie Flehen oder Unterwürfigkeit da diese den Angrei-

fer nur weiter anstacheln. Falls sich in der Umgebung andere Personen befinden, versuche diese anzusprechen.
Wenn du von einer Gruppe Linkskrimineller angegriffen wirst, ist es ratsamer sich zurück zu ziehen. Wenn du auch in einer Gruppe bist und dich trotzdem zurückziehen musst, achte darauf dass ihr geschlossen agiert und niemanden zurück lasst.
Sofort zurückziehen solltest du dich wenn der Angreifer eine Waffe wie z.B. einen Teleskopschlagstock einsetzen will.

2.5 Nach einem Angriff

Hast du dich erfolgreich Verteidigt ist es sinnvoll dich von diesem Ort zu entfernen. Solltest du oder eine Person deiner Gruppe verletzt sein, rufe einen Krankenwagen oder begebt euch in das nächste Krankenhaus und lasst diese Verletzungen verarzten und dokumentieren!
Wenn du wieder zur Ruhe gekommen bist ist es sinnvoll wenn du den Vorfall in einem Gedächtnisprotokoll festhältst.
Das Gedächtnisprotokoll sollte enthalten:

- möglichst genauer Ablauf des Angriffes
- der Ort des Angriffes
- die Anzahl der Angreifer
- Kleidungsmerkmale der Angreifer
- Beleidigungen oder sonstige Äusserungen durch die Angreifer
- vielleicht wiedererkannte Linkskriminelle

Dieses Protokoll solltest du deiner lokalen Kameradschaft oder Aktivistengruppe zukommen lassen. Für Berlin ist es ratsam sich an www.nwbb.org zu wenden.

Einerseits werden dadurch meist mehr Fälle linker Gewalttaten vermerkt, die einer oft getätigten Beschönigung der Zahlen und Fakten widersprechen und zugleich wird damit das immer noch vorhandene Problem linkskriminell-motivierter Gewalt thematisiert.

2.6 Psychologische Aspekte nach einem Angriff

Unruhige Nächte nach einem tätlichen Angriff sind völlig normal. Bei einem „Outing“ kommen oftmals auch noch die Sorgen um die Arbeit und die Familie dazu. Rede mit deinen Kameraden darüber! Erzähle ihnen, wie du dich fühlst! Du brauchst dich nicht zu schämen, wenn du unsicher bist oder angst hast. Die Gruppe muss so etwas verstehen.

Diskutiert zusammen darüber, was ihr in Zukunft machen wollt und wie ihr auf den Angriff reagiert. Eines sollte klar sein: Bei solchen Gesprächen werden die Mobiltelefone ausgeschaltet und ein Ort gesucht, wo euch niemand hört, denn es wäre nicht das erste Mal, dass Kameraden abgehört werden.

Das Schlimmste wäre, sich von linkskriminellen Angriffen mürbe machen zu lassen. Denn genau das beabsichtigen die Antifaschisten, nämlich psychischen und physischen Terror zur Vernichtung des politischen Gegners.
Lass dich nicht unterkriegen! Gemeinsam sind wir stark!

2.7 Umgang mit der Polizei

Sicher stellst du dir die Frage ob du nach einem Angriff die Polizei von diesem Vorfall informieren solltest.
Eine eindeutige Antwort können wir dir nicht geben da wir schon die Erfahrung machen mussten, dass die Strafverfolgungsbehörden am Ende auch gegen das Opfer (also dich) ermittelt haben.

Erfahrungsgemäß lohnt es sich nicht, nach einem linkskriminellen Anschlag die Polizei zu informieren. Eine strafverfolgung der Täter verläuft im Sande, die Ermittlungen werden schlampig geführt und reichen meist nicht zu einer Anzeige. Oft genug kam es bereits vor, dass der Staatsschutz vor dem Tür stand und im Endeffekt nur Informationen über nationale Strukturen ergattern wollte.
Andererseits kann es auch passieren, dass nach einer erstatteten Strafanzeige der oder die Schläger doch gefasst werden und es zu einer Anklage kommt. Wenn du dann einen Anwalt als Geschädigter bzw. Nebenkläger nimmst, bekommst du Akteneinsicht, das heißt unter anderem auch:
Name und Adresse des Angreifers!!

Dennoch: Mit dem Staatsschutz oder Verfassungsschutz gibt es im Nachhinein keine Zusammenarbeit!

2.8 Aussageverweigerung und Verhörmethoden

Eine Festnahme, ein Verhör oder eine Hausdurchsuchung trifft dich fast immer unvorbereitet. Das gehört bereits zur erfolgsgerichteten Taktik der Polizei. In dieser Situation hat sie dir gegenüber folgende Vorteile:

- Für dich ist diese Situation eine Ausnahme - für sie ist es eine Routine.
- Du bist von Personen deines Vertrauens abgeschnitten.
- Die Beamten haben ständig die Möglichkeit, bei veränderter neuer Lage neue Instruktionen einzuholen.
- Du kennst deine Rechte nur unvollkommen, sie wissen das.
- Du bist nervös und aufgeregt. Sie sind gelassen und darauf getrimmt, deine Nervosität zu ihren Gunsten auszunutzen.
- Du weißt nicht, was sie mit dir machen werden und wie lange das Verhör dauert und was es ergibt - sie haben davon eine genaue Vorstellung.
- Du bist ausgeliefert und fühlst dich entsprechend schlecht. Die Angst und die Ungewissheit machen dich fertig - sie rechnen damit.

In dieser Situation sind viele bereit, auf alle gesetzlich garantierten Rechte, im besonderen auf Aussageverweigerung, zu verzichten. Für den Wunsch „nur raus hier und es hinter mir haben“, sind manche schon für Jahre ins Gefängnis gewandert, weil sie ihr Recht auf Schweigen nicht mehr wahren konnten. In dieser Lage bist du nicht Herr des Verfahrens. Du kannst mit absoluter Sicherheit nicht wissen, ob eine Aussage deine Situation letztendlich verbessert. In dieser Lage kannst du nur spekulieren. Spekulation ist Abenteurerei.

Es gibt keine Situation, in der du eine Aussage nicht auch noch in 14 Tagen machen könntest!

Wichtig ist, die Mechanismen zu kennen, die Menschen zum Reden bringen. Eine Vernehmung ist kein Spiel von Frage und Antwort. Sie ist zunächst eine Situation, in der man nicht nur bewusst und vernünftig handelt, sondern vor allem von unbewussten Regungen, teilweise mechanisch, gesteuert wird. Der geübte Kriminalbeamte wird, wenn der dich schon kennt, bereits von Anfang an

diese Regungen und Verhaltensweisen an dir studieren. So kann er im Verlauf der Handlungen in deinem Unterbewusstsein Reaktionen auslösen, die ihn seinen Zielen näher bringen. Viele begreifen später nicht, wie es zu Aussagen kommen konnte.

Warum ist es richtig, nichts zu sagen, bevor man nicht mit seinem Anwalt gesprochen hat?

Das Gesetz gibt dir als Beschuldigter das Recht, dich selber nicht zu belasten. Das gleiche gilt für den Zeugen unter den oben genannten Voraussetzungen. Es gibt vor allem nach einer Festnahme keine Situation, in der du sachlich und juristisch beurteilen kannst, ob deine Angaben tatsächlich einen Vorteil für dich bringen. Du weißt gar nicht, an welcher Stelle des Verfahrens du bist. Dir fehlt der Lotse. Frag erst einen Anwalt! Wenn er nicht erreichbar ist, warte mit allem, bis du ihn erreicht hast und er kommen kann. Mach dir unter keinen Umständen die Ungeduld und Eile des Beamten zu eigen. Wenn er es eilig hat, hast du gerade Zeit. Und nimm bloß nicht ihn etwa als Lotsen. Du kannst dir hoffentlich denken, dass er dich nicht in deinem Interesse, sondern in seinem lotst.

Der Polizeibeamte hat nur ein Ziel: Seinem Vorgesetzten ein Ergebnis zu präsentieren. Du bist ihm letztlich scheißegal! Wenn du aufgrund deiner Aussage noch im Knast sitzt, ist er dafür vielleicht schon befördert worden. Deine Rechte nach einer Festnahme:

- den Grund für die Festnahme zu erfahren
- alle Aussagen zu verweigern
- nichts zu unterschreiben
- gegen eine erkennungsdienstliche Behandlung schriftlich Widerspruch einzulegen
- im Verletzungsfalle einen Arzt zu verlangen und die Verletzung attestieren zu lassen
- ein Protokoll über die beschlagnahmten Sachen zu erhalten
- einen Anwalt anzurufen und nächste Angehörige zu benachrichtigen (Aber nicht unnötig am Telefon quasseln)

2.9 Die prozessuale Bedeutung der Aussageverweigerung

Dein Schweigen hat auch eine prozessuale Bedeutung. Nur die totale Aussageverweigerung darf bei einem Beschuldigten nicht zu seinem Nachteil gewertet werden. Sagst du nur ein Wort, so wird dies zu einem Beweismittel, das nach der Rechtssprechung der tatrichterlichen Beweiswürdigung unterliegt. Beispiel:

Du wirst gefragt, wo du im August 1998 warst. Wenn du bisher weder auf diese noch auf eine andere Frage geantwortet hast, kann dein Schweigen nicht verwertet werden. Sagst du aber nur: „Am 17.August habe ich demonstriert“ (vielleicht, weil man dir ein Foto vorhält, auf dem du zu sehen bist), so kann daraus der Schluss gezogen werden, dass du an diesem oder jenem Ort warst und dieses oder jenes getan hast.

Solange du keinen Lotsen hast hilft dir nur konsequentes Schweigen!

Eine getätigte Aussage kannst du nicht mehr widerrufen. Man kann nur einer Aussage eine weitere hinzufügen, die vom Inhalt der Ersten abweicht. Das Gericht ist dann in seiner Wertung frei, welcher es Glauben schenkt. Meist werden die Beamten, welche die Aussage zustande gebracht haben, in der Verhandlung vernommen, und die werden ihr übriges tun, die geeignete Aussage dem Gericht mundgerecht zu machen.

2.10 Warum ist es wichtig, mit einem Anwalt zu sprechen?

Das Gesetz gibt dir als Beschuldigten das Recht, dich selber nicht zu belasten. Das gleiche gilt für den Zeugen. Es gibt vor allem nach einer Festnahme keine Situation, in der du sachlich und juristisch beurteilen kannst, ob deine Angaben tatsächlich einen Vorteil für dich bringen. Du weißt gar nicht, an welcher Stelle des Verfahrens du bist. Dir fehlt der Lotse - Frag also erst einen Anwalt.

Wenn er nicht erreichbar ist, warte mit allem, bis du ihn erreicht hast und er kommen kann. Mach dir unter keinen Umständen die Geduld und Eile des Beamten zu eigen. Wenn er es eilig hat, hast du gerade Zeit. Und nimm bloß nicht ihn etwa als Lotsen! Du kannst dir hoffentlich denken, dass er dich nicht in deinem Interesse, sondern in seinem lotst.

2.11 Die Aussageverweigerung als Zeuge

Polizei:
Einer Ladung zur Polizei (auch beim LKA) brauchen weder Beschuldigte noch Zeugen Folge zu leisten. Es entstehen dadurch keinerlei Nachteile (auch wenn es einem der schwer verständliche Juristentext der Vorladung suggerieren will). Auf eine Ladung sollte man in keiner Weise reagieren, also auch nie telefonisch absagen, auch wenn darum in der Ladung gebeten wird. Bei dieser Gelegenheit wird man nämlich nochmal vollgesülzt. Sofort müssen allerdings Freunde, Mitbetroffene, Anwälte ... informiert werden!

Staatsanwalt:
Zeugen müssen vor dem Staatsanwalt erscheinen und die Angaben zur Person machen. Erscheinen Zeugen nicht, kann eine Vorführung erlassen werden.

Sodann hat man das Recht, folgendes zu erfahren: Um welches Verfahren es sich handelt (hier ist auf eine genaue Bezeichnung der einzelnen Tatvorwürfe zu bestehen). Der/die Beschuldigten müssen genannt werden. Denn man muss ja die Möglichkeit haben, zu prüfen, ob man ein Aussageverweigerungsrecht hat.

Es gibt gute Gründe, warum Zeugen vor dem Staatsanwalt nicht aussagen wollen. Sie können zu diesem Zeitpunkt nicht ermessen, wozu ihre Aussagen verwendet werden. Sie wissen nicht sicher, in welche Richtung der Staatsanwalt ermittelt, der Staatsanwalt darf Zeugen darüber auch weitgehend in Unkenntnis halten - und auch darüber, ab wann in seinen Augen eine Aussage die Zeugen selbst belasten könnte! Ein Überblick über die Zusammenhänge, in der die Aussagen stehen, dürfte für die Zeugen unmöglich sein. Jede Aussage beim Staatsanwalt liefert ein Steinchen in dem Mosaik, dass er sich zusammenbastelt, jede Aussage kann ihm dabei weitere Anhaltspunkte liefern. Das Aussageverweigerungsrecht für Zeugen wird durch die § 52 bis 56 der Strafprozessordnung (StPO) geregelt.
§ 52 StPO sieht ein Aussageverweigerungsrecht für Verwandte des Beschuldigten vor, dass können sein, Eltern, Geschwister, Kinder, aber auch Verlobte ...
Verlobungen sind bekanntlich ebenso schnell zu lösen, wie sie geschlossen werden, und können im Einzelfall, wenn es möglich ist, eine sehr elegante Lösung sein.
§ 55 StPO sieht ein Aussageverweigerungsrecht vor für Leute, die in derselben Sache angeklagt sind und für Leute, die sich durch die Aussage selbst belasten könnten. Es ist sowohl taktisch wie politisch falsch, diese Form der Aussageverweigerung zu benutzen. Die Aussageverweigerung nach § 55 besteht nur für spezielle Fragen. Die Inanspruchnahme dieses Rechtes muss jeweils ausdrücklich, unter Berufung auf die Gefahr der Selbstbelastung verlangt werden. Die Gefahren dabei liegen auf der Hand: Zum einen wird die Staatsanwaltschaft verlangen, dass begründet werden muss, wieso man sich selbst belasten könnte ... dabei entsteht zwangsläufig die Situation, dass man über die Anklagepunkte reden muss oder über Leute, mit denen man irgendwie zu tun hat. Überlegungen welche Aussagen dem Staatsschutz nützlich sein können, und welche nicht, führen zu einer Situation, die für die Betroffenen nicht mehr überschaubar ist. Sie können

immer wieder vorgeladen werden - die Bedrohung, vom Zeugen zum Beschuldigten zu werden, immer im Hinterkopf, was immer wieder eine Entscheidung fordert, wie sie schon bei der ersten Vorladung zu treffen war. Taktisch ist die Berufung auf den § 55 unklug, da man durch diese Begründung quasi der Justiz die Möglichkeit in die Hand gibt, einen zum Beschuldigten zu machen, also ebenfalls ein Ermittlungsverfahren einzuleiten denn es ist ja davon auszugehen, dass ein Straftatbestand/Ordnungswidrigkeit vorliegt. Wird man als Zeuge vorgeladen und es ist zu erwarten dass er selbst noch ein Verfahren kriegt oder er weiß es schon, hat man das Recht, auch die Aussage als Zeuge zu verweigern. Dies gilt für das gesamte Verhör.

Erwähnt sei noch, dass Ärzte, Rechtsanwälte, Pfaffen und Journalisten ebenfalls ein begrenztes Aussageverweigerungsrecht haben, welches sich natürlich nur auf ihren Berufsbereich bezieht (§ 53 und 54 StPO). So müssen z.B. Journalisten die Namen von Informanten und Interviewpartnern nicht preisgeben.

Was geschieht mit Personen die die Aussage verweigern wollen, obwohl sie keinen der genannten Paragraphen können bzw. wollen? Oder mit Zeugen, die einer staatsanwaltschaftlichen Ladung nicht folgen wollen?

Dafür werden erst mal die entstandenen Kosten aufgedrückt. Dazu kann der Staatsanwalt ein Ordnungsgeld erlassen. Wenn dieses nicht gezahlt wird, gibt es Ordnungshaft, maximal 42 Tage und nur durch richterlichen Beschluss. Es kann die zwangsweise Vorführung vor einem Vernehmungsrichter (Ermittlungsrichter) angeordnet werden. Die Ordnungsmittel können bei erneutem Ausbleiben wiederholt werden.

Zeugen, die hingehen, aber nichts sagen:

Zunächst läuft alles so wie oben beschrieben ab. Wichtiger Unterschied aber ist, dass damit die Ordnungsmittel verbraucht, also nicht wiederholbar sind! Möglicherweise beantragt der Staatsanwalt nun die Erzwingungshaft (Beugehaft). Wird diese durchgesetzt, ist danach auch dieses Erzwingungsmittel verbraucht. Die Beugehaft kann maximal sechs Monate verhän
gt werden. Klar ist demnach: So schnell ist man als aussageverweigernder Zeuge nicht im Knast! Das geht erst mal alles seinen langen rechtlichen Gang. Zuallererst müssen zunächst einmal die Ordnungsmittel angewandt werden. Staatsanwälte, die behaupten, der Zeuge könne jetzt gleich in Beugehaft gesteckt werden, vermischen bewusst Ordnungs- mit Erzwingungsmitteln um den Zeugen zu verunsichern.

Aussageverweigerung als Zeuge beim Richter:

Alles wie bei dem Punkt Staatsanwaltschaft. Hinzu kommt, dass die Eidesverweigerung ebenso behandelt wird wie eine Aussageverweigerung (siehe auch Abschnitt Falschaussagen). Zeugen können zu allen Vernehmungen Anwälte mitnehmen. Sie können eine wichtige, auch psychologische Funktion haben, doch sollten ihre Möglichkeiten nicht überschätzt werden. Sie haben lediglich die Funktion eines Rechtsbeistandes, d.h. sie können nicht in die Vernehmung eingreifen, sie dürfen nur bei formalen Fehlern des Vernehmenden eingreifen. Wenn z.B. eine Frage juristisch nicht so gestellt werden darf, wie sie gestellt wurde, oder wenn der Staatsanwalt keine Rechtsmittelbelehrung erteilt hat. Aber man hat das Recht, sich mit dem Anwalt über die gerade gestellte Frage im Nebenzimmer zu beraten. Dadurch kann man sich erst mal Luft verschaffen und sich dem psychischen Druck entziehen. Welche sich stark genug fühlen können hiermit das Verhör etwas strecken...

2.12 Die Aussageverweigerung als Beschuldigter

Im Gegensatz zum Zeugen hat ein Beschuldigter das Recht auf eine generelle Aussageverweigerung sowohl bei der Polizei, wie beim Staatsanwalt, als auch vor Gericht. Erscheinungspflicht besteht

für einen Beschuldigten nur bei Gericht.

Polizei:

Für den/die Beschuldigten ist der Druck, der durch eine Verhörsituation und durch die Bedrohung mit Knast entsteht, das zentrale Problem. Die Verhörsituation kann nie vollständig vorherberechnet und geplant werden, eine Selbstbestimmung, die Meinung, man könne irgendwie aus dem Objektstatus, der ihm/ihr zugewiesen wird, ausbrechen, ist Illusion. Uns erscheint wichtig genau um die eigenen Rechte, sowie um mögliche Tricks der Repression zu wissen, und dadurch - einen eventuellen Überraschungseffekt kleinzuhalten.

Es ist auch so, dass etwa bei einem polizeilichen Verhör der Objektstatus von den Polizisten aus, aufgebrochen wird. Man kann nicht einfach dasitzen und sein Maul halten, man will seine Angehörigen sprechen, seinen Anwalt sprechen, braucht vielleicht einen Arzt ... und die Polizisten sind die letzten, die sich darum einen Kopf machen. Die Wahrnehmung seiner Rechte fällt auf einen selbst zurück. Ständig muss man sich verhalten, aktiv werden ... es ist eine Falle unter vielen, die uns die Repression stellt. Dagegen hilft nur das Wissen wo die Grenze zu ziehen ist, wann man das Maul halten muss - also auch hier ist eine vorherige Auseinandersetzung um diese „Aspekte der Aussageverweigerung“ dringend geboten. Es darf nur die generelle Aussageverweigerung nicht zum Nachteil des Beschuldigten gewertet werden!

Das bedeutet:
Macht ein Beschuldigter auch nur eine einzige Aussage (egal. wo) und sei sie noch so unbedeutend, so öffnet er Richtern und Staatsanwälten Tür und Tor, die ansonsten beibehaltene Aussageverweigerung gegen sie/ihn zu verwenden.

Für den Richter heißt dies „freie richterliche Beweiswürdigung“, der jede Aussage unterliegt. Das heißt er kann also bei wenigen Aussagen spekulieren, warum der/die Beschuldigten auf die anderen Fragen nun gerade nichts sagen wollte! Was also bedeutet, dass es Teilaussagen in diesem Sinne gar nicht gibt! Welche auf bestimmte Fragen antworten, sich bei anderen aber auf ihr Aussageverweigerungsrecht berufen, liefern damit immer ein vollständiges Bild von sich selbst.

Ob sie ansonsten schweigen:
Welche einmal geredet haben, liefern Zusammenhänge, einen Kontext, den sich kein Staatsanwalt entgehen lassen wird!

Nach einer Festnahme und vor Gericht sind Beschuldigte zu folgenden Angaben zu ihrer Person verpflichtet:

- Name
- Adresse
- Geburtsdatum
- Geburtsort
- allgemeine Berufsangabe! (z.B. Schüler, Angestellter, Selbstständig. Also nicht der Arbeitgeber.

Jugendliche müssen auch nicht die Adresse der Eltern angeben, wenn sie nicht mehr bei ihnen wohnen. Wer das nicht tut, hat vor Gericht meist mit einem Ordnungsgeld (25 Euro etwa) zu rechnen. Weitere Sanktionen (Ordnungshaft) können folgen. Wer bei der Polizei diese Angaben verweigert, begeht das Delikt der Personalienverweigerung, welches wiederum verfolgt werden kann. Auf jeden Fall kann man durch Beharrlichkeit und dem Verlangen nach dem Einsatzleiter bei einer bloßen

Personalienfeststellung (nicht nach einer Festnahme!) manchmal erreichen, dass diese nicht durchgeführt wird.

Haftrichter:

Es gibt einen Ort, wo eine Aussage angebracht scheint, nämlich vor dem Haftrichter. Hier ist zunächst zu betonen: Eine Aussage zur Sache wendet keine U-Haft ab!

Der Haftrichter erlässt den Haftbefehl wegen „dringenden Tatverdachts“. Egal, was du zu den Tatvorwürfen zu sagen hast und wenn es ein Alibi ist, auf keinen Fall kommst du raus! Zu den Tatvorwürfen, die auf den Ermittlungen der Polizei beruhen, und die zum Haftbefehl führen, kommen noch sogenannte Haftgründe hinzu. Der Haftbefehl kann, wenn die Haftgründe nicht zutreffen, außer Vollzug gesetzt werden, d.h. aber nicht, dass damit auch die Tatvorwürfe aus der Welt wären! Was also die völlige Unsinnigkeit von Aussagen zur Sache vor dem Haftrichter zeigt.

Haftgründe gibt es vier:

- Fluchtgefahr
- Verdunklungsgefahr
- Wiederholungsgefahr
- und besonders schwere Tatvorwürfe.

Bei Vorwürfen, wie Mord, Totschlag und §129 wird grundsätzlich Haftbefehl erlassen. Zu den anderen Haftgründen kann ein Beschuldigter Stellung nehmen. Dies sollte man nur zum Punkt Fluchtgefahr tun!! Sagt man etwas zu den Punkten Verdunkelungs - und Wiederholungsgefahr, ist unweigerlich eine Diskussion über den Tatvorwurf die Folge.

Zum Punkt Fluchtgefahr: Hier sollte man verweisen auf einen festen Wohnsitz, eine Arbeit und andere Bindungen wie z.B. Kinder, langjährige Freundin. Die Gefahr hierbei liegt auf der Hand: dass man nämlich Namen nennt. Es ist also zumindest aufzupassen, wen man nennt. Ganz vermeiden lassen wird sich die Namensnennung sicher nie - es scheint angebracht, sich hierüber schon vorher klar zu werden und mit den u.U. Betroffenen darüber zu reden. Desweiteren halten wir es gerade auch wegen dieser Gefahren für nötig, schon vorher einen Anwalt einzuschalten, der in der konkreten Situation beraten kann.

Klar sein muss man sich aber unbedingt darüber, dass mit einer Aussage zur Sache keine U-Haft abgewendet werden kann. Der Haftrichter ist nun wirklich der letzte Ort, wo eine Aussage „nützt“.

2.13 Die Vernehmungstaktiken

Nach erfolgter Festnahme - im Gefangenentransportwagen, in der Polizeizelle bei der Kripo - setzen irgendwann die Versuche ein, Aussagen zur Sache aus dir herauszuquetschen.

Die Informationen, die Beamte benötigen, haben zweierlei Charakter:

- Sie sollen in einem Strafverfahren verwendet werden, müssen also gerichtsverwertbar sein, d.h. sie dürfen nicht unter Umgehung von Gesetzen, z.B. dem § 136 StPO, zustande kommen.
- Sie sollen der weiteren Ermittlungsarbeit dienen. Hier darf die Ermittlungsbehörde jeden Hinweis verwerten. Hier wird zum Beispiel das Telefon eines Arztes abgehört, nur darf ein sich daraus ergebener Hinweis nicht im Verfahren verwertet werden. Wird aber aufgrund

dieser widerrechtlich erlangten Informationen eine Hausdurchsuchung durchgeführt, so ist das hierdurch sichergestellte Material verwertbar.

Willst du also deine Rechte voll wahren, musst du sorgfältig darauf achten, dass Informationen, die du im Kopf hast, auf keinem Wege denselben verlassen. Das Gesetz geht von der Fiktion aus, der Mensch habe einen freien Willen, den er nach Belieben betätigen könne, auch der Entschluss gemäß § 136 auszusagen, sei frei, wenn er nicht unter den besonderen Umständen des § 136 StPO zustande gekommen ist.

Die Beamten werden dir also zunächst die gesetzlich zulässige Entscheidungshilfe geben wollen. Dazu werden sie aus ihrer Maske als Kriminalbeamte heraus schlüpfen und versuchen, dir gegenüber die Rolle "Deines Anwaltesßu spielen. Anstatt dir sofort Gelegenheit zu geben, wirklich deinen Anwalt zu befragen, haben sie ein Interesse daran, diesen zunächst fern von dir zu halten.

Sie werden alle Register ziehen, um deinen freien Willen in ihre Richtung zu lenken.

2.14 Die Taktik des - Es Ist Das Beste Für Dich

Sie werden versuchen, dir weiszumachen, das Beste für dich sei, auszusagen. Das geschieht, indem man dir vorhält, welche Strafen einen erwarten. Sie werden dir weiszumachen versuchen, deine Position sei ohnehin aussichtslos. Der Geständige aber erhalte Straferlass und komme möglicherweise nicht in die Untersuchungshaft, weil dann keine Verdunklungsgefahr bestehe.

Wenn sie Recht hätten, bräuchten sie die Zuziehung eines Anwaltes nicht zu fürchten. Es muss dich misstrauisch machen, dass sie dir raten wollen, es aber nicht zulassen, dass dies eine Person deines Vertrauens tut.

Nochmal:
Die Vernehmung ist nicht nur ein Spiel von Fragen und Antworten, sondern eine Situation, zu der nicht nur der Beamte und Befragte gehört, sondern ebenso deine Angst, seine Routine, die Wahl des Zimmers, die Beamten, die scheinbar nicht beteiligt sind, Hektik, Ungeduld und gespielte Szenen.

Der Beamte wird zunächst versuchen, mit dir ins Gespräch zu kommen.

Man wird dir Ermittlungsergebnisse vorlesen, die dir zeigen sollen, wie weit man mit den Ermittlungen ist. Du kannst aber gar nicht beurteilen, ob dies tatsächlich Ergebnisse oder nur Vermutungen sind. Es ist vorgekommen, dass dem Beschuldigten Papiere als „Geständnisse“ vermeintlicher Mitbeschuldigter vorgelegt wurden, an denen kein Buchstabe echt war. Abgesehen davon, ist auch ein wirkliches Geständnis noch lange kein Grund, auf sein Schweigerecht zu verzichten, denn nur ein Anwalt kann beurteilen, ob dieses vermeintliche Geständnis echt ist. Weiter wird man versuchen, dich mit Namen, Adressen, Telefonnummern und Tatsachen aus deinem Leben, von denen du meinst, sie seien unbekannt, zu überrumpeln.

Durchschaue diese Manöver. Wenn sie alles wissen, wozu dann noch eine Aussage. Wenn du bereits überführt wärest, wie wollen sie dir dann eine milde Strafe versprechen? Darüber entscheidet ohnehin das Gericht, das dir gewiss nicht dankbar ist. Wenn sie in der Rolle deines Anwaltes keinen Erfolg haben oder wenn sie merken, dass du dir von ihnen nichts einreden lässt, werden sie versuchen, dich psychisch zu bearbeiten.

2.15 Die Taktik, Kameraden gegeneinander auszuspielen

Fall nicht darauf rein, wenn man dich zusammen mit anderen Gefangenen oder sogar mit Kameraden transportiert, warten lässt oder gemeinsam vernehmen will. Das ist nur ein weiterer Versuch,

Aussagen von dir zu bekommen, auf die die Gegenseite schon lange wartet. In dieser Situation gibt es zwei Möglichkeiten:

Du kennst den anderen (natürlich nicht richtig, sondern einigermaßen gut). Dann vermeide jede Geste des Wiedererkennens. Oft ist bereits so etwas Gegenstand von Ermittlungen. Fallt euch nicht um den Hals. Fragt nicht nach dem Tun der letzten Zeit. Sprecht nicht von früher. Sprecht auch nicht, wenn ihr alleine seid über Dinge, die die Polizeibeamten mithören könnten. Wenn er Durchblick hat, begreift er es. Wenn nicht, ist es um so gefährlicher.

Auch hier gilt es, dass es besser ist, jemanden vor den Kopf zu stoßen und es später mal zu erklären, als sich und andere um seine Rechte und in Gefahr zu bringen.

Du kennst den Anderen nicht. Dann sprich nicht über dich, sondern nur über ihn. Gib keine Kommentare. Sprich über das Wetter, den Knast, Essen und Sport. Auf keinen Fall über deinen Fall. Vermeide auch hier Imponiergehabe. Hab den Mut, für ein Würstchen gehalten zu werden. Wenn du wieder draußen bist, werden sie wissen, dass du keines warst. Denk daran, dass sie auch Pannen spielen können. Es ist durchaus möglich, dass sie dich „versehentlich“ mit jemanden zusammentun, von dem sie dich vorher streng isoliert haben. Deine Freude musst du dann zügeln. Verhalte dich so, dass sie aus deinem Verhalten keinerlei Informationen ziehen können. Was für Begegnungen mit Personen gilt, trifft auch auf Orte oder Sachen zu. Nicht selten wird ein Betroffener an Orte gefahren, von denen angenommen wird, dass er sie kennt. Die Polizeibeamten wollen an der Reaktion prüfen, ob sie mit bestimmten Vermutungen auf dem richtigen Weg sind. Richte dein Verhalten danach ein. Werde nicht plötzlich in einer bekannten Gegend munter und recke den Hals, wenn du vorher geschlafen hast. Gib keine Hinweise auf Ort - oder Wegkenntnisse.

Wenn man dir Sachen, wie Waffen, Kleidung, Schlüssel, Autos oder sonst etwas zeigt, zeige für nichts davon Interesse. Nimm auch nichts davon in die Hand. Man kann aus der Art, wie jemand etwas anfasst, sehr gut sehen, ob er gewohnt ist, damit umzugehen.

2.16 Die Taktik des - Sie Haben Gewonnen

Eine weitere Gefahrenquelle ist die Euphorie, die sich einstellt, wenn man meint: Ich habe es geschafft.

Fast jeder weiss, wie man sich fühlt, wenn man aus einer Drucksituation befreit wird. Man ist gesprächig, fröhlich und redet wie aufgedreht, z.B. wenn man eine Klassenarbeit, eine Klausur oder eine Prüfung erfolgreich hinter sich hat. Man fühlt sich unbeschwert, wenn man die Last los ist. In dieser Stimmung hat man wenig Lust, noch weiter an die Strapazen zu denken. Man vergisst schnell die Mühsal und damit leider auch jede Vorsicht.

Nach einer langwierigen Druckperiode in einem Vernehmungszimmer, nach allen möglichen Beschimpfungen, Anfeindungen und all den Strapazen wird plötzlich gesagt: Schluss, es hat keinen Zweck, er will nicht, gut. „Sie haben gewonnen.“, sagt ein Beamter zu dir. Du bist froh, stolz und weißt, dass du gut warst. Warst du auch.

Aber Schluss ist eben nicht dann, wenn sie es sagen. Jetzt beginnt ein neuer Rollenwechsel. Du siehst die Beamten, mit denen du zu tun hattest, erschöpft. Sie waren erfolglos. Sie übergeben dich jetzt einen anderen, den du noch nicht kennst. Der hat nur den Auftrag, mit dir etwas zu essen, oder dich ins Gefängnis zurückzubringen. Er scheint völlig unverdächtig. Er fragt dich, ob du sie fertiggemacht hast. Er spielt Schadenfreude. Du freust dich, dass du jemanden hast, der deine Freude teilt - aber auch er wartet nur auf deine Worte.

2.17 Psychischer Druck und Entspannung

Bereits im Transportwagen in der Polizeizelle oder bei der Kripo, wenn es dir bereits besonders dreckig geht, wird ein Beamter in der Rolle des FFreund und Helferäuf dich zukommen. Das kann ein „Höherer“ sein, der die Polizisten, die dich beschimpfen, zur „Ordnung“ ruft. In deiner miesen Situation neigst du dazu, dich an diesen Strohhalm zu klammern und zu vergessen, dass er derjenige ist, der jetzt den Auftrag hat mit dir in ein vertrauensvolles Gespräch zu kommen.
Es passiert nicht selten, dass gerade dieser Beamte sich später vor Gericht rühmt, er habe es eben mit seiner verständnisvollen Art geschafft, das Vertrauen des Beschuldigten zu erlangen, der ihm schließlich das Herz ausschüttete. Die Taktik besteht darin, dich zunächst in eine Situation zu bringen, in der es dir schlecht geht, damit dann einer als dein FFreund und Retteräuftreten kann. Oft werden zu diesem Zweck auch Vernehmungen mit verteilten Rollen durchgeführt:

- Einer ist scheinbar der Sachliche, der die Vernehmung offiziell vornehmen soll.
- Zwei weitere Beamte sind im Raum entweder als Zuhörer oder scheinbar mit etwas Anderem beschäftigt.

Du verweigerst die Aussage. Dein sachliches Gegenüber versucht dir in Güte zuzureden. Du schweigst. Er brüllt los: Mit euch müsste man kurzen Prozess machen... Dabei kommt er dir so nahe, dass seine Nase dich fast berührt. Du riechst seinen Atem und bekommst seine Spucke ins Gesicht. Er brüllt weiter, bis nun dem Dritten die Sache „zuviel“ wird. Er schickt den Schreier raus und befreit dich von ihm. Er wird dir sagen, dass sie den auch nicht leiden können, dass er bald versetzt wird. Dann bieten sie dir eine Tasse Kaffee an. Du empfindest Dankbarkeit. Du solltest Dankbarkeit empfinden.

Die Beamten wissen, dass wir in bestimmten Situationen nach Mustern und Mechanismen zu reagieren pflegen. Wir sind einfach darauf gestimmt, jemandem, der uns hilft, dankbar zu sein oder dem, der uns Verständnis entgegenbringt, freundlich zu begegnen. Das muss im normalen täglichen Umgang auch nicht falsch sein. Aber diese eingeschliffenen Mechanismen des täglichen Lebens sind uns so in Fleisch und Blut übergegangen, dass sie auch in Situationen aktiv sind, wo sie überhaupt nicht angebracht sind. Das Verhältnis zwischen Beamten und Beschuldigten ist in keiner Situation geeignet, Freundlichkeit oder Dankbarkeit aufkommen zu lassen. Auch wenn es dir schwer fällt, mit dem Beamten, dem du Dank schuldest, nicht zu sprechen, in ihm immer noch den Systemschergen zu sehen. Vergiss nicht, dass es dein Recht ist, zu schweigen. Wenn der Beamte erst seine Macht darauf verwendet, dich unter Druck zu setzen und dann den Druck lockert, ist es absurd, hierfür auch noch dankbar zu sein. Selbst wenn er den Kaffee aus eigener Tasche bezahlt, ist das eine Investition, die sich für ihn spätestens bei der nächsten Beförderung auszahlt.
Diese Retter sind die gefährlichsten Personen in diesem abgekarteten Spiel. Sie wollen deinen Kopf, deine Aussage und deinen Entschluss zum Geständnis. Du hast zu kämpfen, um ihnen zu widerstehen. Und wenn du meinst, deine Dankbarkeit wirklich nicht verkneifen zu können, kannst du dem Beamten später, wenn du aus der Sache raus bist, immer noch eine Büchse Bier als Dank schicken. Aber keine Aussage! Wenn der Beamte seine „menschliche“ Seite zeigt, verweigere nicht nur jede Aussage, sondern lass dich auf kein Gespräch von Mensch zu Mensch ein. Er wird dir erzählen, dass er auch Kinder hat, die womöglich rechts eingestellt sind. Er findet vieles ja auch richtig und versteht auch die Jugend; er würde ja auch mitmachen.

Er wird versuchen, dich in eine Diskussion zu verwickeln, innerhalb der er dich langsam auf eine Bahn bringen kann, die dann zu einer Aussage Führt. Außerdem verstärkt sich deine emotionale Beziehung zu ihm. Du findest ihn freundlich und fühlst dich verstanden. Das hat zur Folge, dass du bewusst oder unbewusst dich selbst veranlasst fühlst, freundlich zu ihm zu sein und ihn zu verstehen. Du beginnst jetzt Angst zu haben, ihn durch weiteres Verweigern zu „enttäuschen“.

2.18 Aussageverweigerung und Knast/Beugehaft

Die Diskussion um Aussageverweigerung fordert eine ständige Thematisierung von Knast/Beugehaft, keinesfalls darf dieser Punkt ausgeklammert und hier eine Trennung gezogen werden. Angesichts dieses Repressionsmittels wächst bei vielen die Aussagebereitschaft. Die fehlende Thematisierung weist auch auf den Punkt Aussageverweigerung und Organisierung hin, eine Einschätzung der eigenen Struktur hat meist nicht stattgefunden, drum wird auch die Bedrohung mit Knast individualisiert:

Lieber ein paar Jahre in den sicheren Knast, als sich in der Illegalität auf die eigenen, unsicheren Strukturen draußen verlassen. ...

Die Beugehaft (die sich nur auf Zeugen bezieht) steht am Ende einer Reihe von Möglichkeiten der Repression den Aussageverweigernden zunächst mit Geldstrafen bedrohen kann. Nichtsdestotrotz ist sie ein brennpunktartiger Ausschnitt, der die reale Gefahr Knast drastisch vor Augen führt. Die Situation für den Zeugen, als auch für den Beschuldigten ist in Bezug auf den Knast generell dieselbe. Die Beugehaft dient zur Erpressung einer Aussage, Benennung von Tätern. Die persönlichen Folgen der Beugehaft sind eklatant. Neben dem möglichen Verlust des Arbeitsplatzes, der Wohnung, der Beziehungen (und auch des Anspruches auf Arbeitslosengeld) kommen dazu die Sorgen um Kinder und die Anhäufung von Schulden.

Beugehaft ist Zivilstrafe und muss grundsätzlich selbst bezahlt werden! (Tagessatz a 20 Euro) Abstrakt gesagt, hat die Bedrohung des Beschuldigten mit Knast eine ähnliche Funktion. Knast wird eben nicht nur als Sanktion eingesetzt, sondern auch als Erpressungsmittel. Die Bedrohung Knast soll den Beschuldigten zur Kooperation zwingen, diese ihm gleichsam als günstigere Alternative erscheinen. Es herrscht Berührungs- bzw. Auseinandersetzungsangst bezüglich Beugehaft, die Ausdruck einer allgemeinen Verunsicherung ist, die z.B. seiner Zeit in Bochum nach den ersten Beugehaftbeschlüssen einsetzte. Die Überzeugung der Aussageverweigerung als sicherste Verhaltensweise gegenüber Polizei, Staatsanwalt, Staatsschutz etc. wird dabei nicht generell in Zweifel gezogen - nur wird Beugehaft und Aussageverweigerung getrennt behandelt, und wenn überhaupt im Bereich des Individuellen thematisiert. Die Debatten kreisen vordergründig um den Punkt: das Absitzen der Beugehaft ist ein zu hoher Preis für die Aussageverweigerung. Es wird ein Weg zwischen Aussage und Knast gesucht, orientiert wird sich dabei an den persönlichen Folgen. Die politische Konsequenz oder Funktion von Aussageverweigerung wird dabei übergangen. Das Standhalten, bzw. Nachgeben gegenüber Knast/Beugehaft werden zum persönlichen Problem, mit dem sich die Betroffenen herumzuschlagen haben, was der politischen Notwendigkeit der Aussageverweigerung eklatant widerspricht. Fatal - aber auch bezeichnend - ist die Tatsache, dass die Auseinandersetzung um die Beugehaft dann beginnt, wenn Beugehaftbeschlüsse vorliegen - um zu versiegen, wenn die Leute wieder aus dem Knast sind, was doch ein Ausdruck einer Hilflosigkeit ist. Das Wissen um die eigene Erpressbarkeit, die Angst vor Knast und den Folgen, sowie die politische Schwäche, sind für viele Richtlinie ihres Handelns, was zum wiederholten Male auf das Kernproblem Organisierung stößt. Aus unsicherer Haltung heraus wird der Zweifel an die grundsätzliche politische Funktion der Aussageverweigerung sichtbar. Taktisches Kalkül tritt an die Stelle einer konsequenten Aussageverweigerung.

Da wo es mehrere Vorladungen gab, ist eine gemeinsame Vorbereitung noch notwendiger. Diese erfordert entsprechende Bereitschaft, sich mit den eigenen Schwächen, sowie auch mit den direkt Verfolgten zu konfrontieren und darüber hinaus die Bestimmung einer inhaltlichen politischen Position. Es ist wichtig, eine gemeinsame Plattform zu schaffen, aus der sich als logische Folge kollektive Aussageverweigerung ergibt. Die Auseinandersetzung um Knast, persönliche Situation (auch emotionale) und um das Machbare ist auch hier von Nöten um die Lücke zwischen abstrakter politischer Bestimmung und persönlicher Konsequenz zu schließen.... Es ist unwahrscheinlich, ein kollektives Vorgehen in allen Details zu praktizieren. Es lässt sich nicht alles trainieren und vorausbestimmen. Der Druck auf die Einzelnen bezüglich der Beugehaft ist unterschiedlich. Deshalb

erscheint uns also als außerordentlich wichtig eine gemeinsame inhaltliche politische Bestimmung. Sie erfordert von allen ein dem gemäßes Verhalten und dass nicht alles auf die Betroffenen abgeladen wird, diesen mit falscher, nur fordernder und nehmenden Solidarität der Boden unter den Füßen weggezogen wird.

2.19 Falschaussagen

Tatbestand: Falsche uneidliche Aussage
Strafrahmen: 3 Monate bis 5 Jahre. Meineid: nicht unter 1 Jahr.

Ein Beschuldigter darf überall lügen, ein Zeuge hingegen ist vor Gericht zu wahrheitsgemäßer Aussage verpflichtet. Beim Staatsanwalt gibt es zwar keinen Tatbestand der Falschaussage, möglich ist jedoch, dass durch eine Falschaussage der Straftatbestand der Strafvereitelung erfüllt wird! - Auch deshalb halten wir generell wenig von Falschaussagen. Sie sind immer ein Wagnis, und können zu Verstrickungen oder gar zu Namensnennungen führen. Die Bullen sind aber da nicht blöd, wo sie es sich nicht leisten können. Angesichts ihrer Möglichkeiten, gerade auch technischer Art können Falschaussagen geradezu zu einer immensen Gefahr werden!

2.20 Alibiaussagen

Das Fiktive Beispiel:

Vor dem Landgericht ist ein 28 Jähriger Maurer angeklagt, im Zusammenhang mit einer Demonstration den Rechten Arm zum Hitlergruss gehoben zu haben. Er wird kurze Zeit nach der angeblichen Tat von einem Beamten wiedererkannt (an seinem auffälligen Hemd) und verhaftet. Eine Stunde wird er in der Wanne gefangenhalten und muß sich - im rechtsfreien Raum, die üblichen üblen Sprüche anhören. Sodann wird er zwei Stunden von einem Staatsschutzbullen verhört. Der Beschuldigte weiß, daß er zur Tatzeit noch zu Hause war, weit entfernt vorm angeblichen Tatort. Er benennt zwei Freunde als Zeugen für sein Alibi. Der Trick der Bullen:
Die beiden Freunde werden nicht sofort verhört - was auch eher sehr unangenehm hätte werden können - sondern erst zwei Wochen später vorgeladen!

Dieser Zeitraum diente denn dem Staatsanwalt dazu, die Aussagen der beiden vor Gericht als abgesprochen zu bezeichnen.

Dieses Beispiel zeigt zunächst, wie schnell du in so eine Situation geraten kannst. Es zeigt dann, dass ein Alibi, im Bewußtsein seiner „Unschuld“ geäußert, keinerlei Gewähr bietet. Ob Alibi oder nicht, die Bullen wollen nur eins: daß geredet wird! Namen, Namen! - der Rest wird sich dann schon finden.

Da zeigt sich, dass ein Rechtsverständnis bürgerlicher Kreise „aber ich bin doch unschuldig“ für die Beamten völlig unerheblich, ja fast lächerlich naiv angesichts der Realiltät ist. Die Unschuld interessiert doch die Justiz immer als letztes! Diese Einsicht verringert schlagartig die Hoffnung die du in Aussagen, Kooperation setzt - aber sie muß ersteinmal vorhanden sein!

2.21 Entlastungszeugen

Ein Bereich, den wir als äußerst problematisch ansehen. Einerseits kann auch eine gute Verteidigung nicht auf entlastende Zeugen verzichten. Andererseits solltest du deren Stellenwert nicht überschätzen: ein Bullenzeuge, der seine Aussage wenigstens halbwegs auf die Reihe kriegt - und wenns nur ein „der/die wars!“ ist - reicht allemal hin.

Daneben lauern auch auf Entlastungszeugen Gefahren, über die vorher Bewußtsein hergestellt werden muss.

Wir haben poplige Beleidigungsprozesse erlebt, in denen es um Geldstrafen ging und bei dem z.B. einem Entlastungszeugen nacheinander folgende Fragen gestellt wurden: Gehen Sie öfter auf Demonstrationen? Waren Sie auch bei der und der Aktion dabei? ...

Aussagen bei Gericht bieten die Möglichkeit der Vorbereitung, Zuschauer können sie verfolgen, Klarheit wird so gewährleistet. Eine gemeinsame Diskussion über Sinn und Zweck von Aussagen vor Gericht ist möglich und überdies unbedingt notwendig, um dem Angeklagten keinen Bärendienst zu erweisen. Gerichtsaussagen verlangen also eine gemeinsame praktische und politische Bestimmung, die von Fall zu Fall neu überdacht werden muss. Eine generelle, schlagwortartige Formulierung läßt sich hier u.E. nicht aufstellen.

2.22 Erfahrungsbericht: Die Vernehmung

Als sie mich am nächsten Tag zur Vernehmung holen, bin ich froh, aus meiner Zelle herauszukommen. Ich bin froh, Menschen zu sehen, freundliche Gesichter, und als sie mir eine Zigarette anbieten, rutscht mir ganz automatisch ein „Danke“ von den Lippen. Da ist ein helles Bürozimmer, Blumentöpfe, eine Sekretärin kocht Kaffee und schon bist du eingestimmt auf ein normales - „Mensch zu Mensch“ Verhalten. Du willst niemanden vor den Kopf stoßen. Es fällt mir schwer, auf ihre freundlichen Fragen nicht zu antworten, und ich hatte mir die Polizisten ganz anders vorgestellt. Der eine ist jung und hat kurze Haare; der andere ist graumeliert, braungebrannt und ganz väterlich. Sie wollen nichts weiter als sich mit dir ein bisschen unterhalten.

Ohne Protokoll und Tonband sagen sie; sie wollen nur wissen, was wir so denken. „Es muss ja was dran sein, wenn man sich jahrelang für eine Sache einsperren lässt.“ Sie sind ja auch nicht mit allem zufrieden, die vielen Ausländer, die Umweltzerstörung, da müssten wir doch mal was machen. Und dann gibts ja heute so viele Gruppen und Parteien, da findet sich ja kein Mensch mehr zurecht. Der Ältere war noch in der HJ und er hat gute Erinnerungen daran. Damals war noch Disziplin in Deutschland. Der Jüngere sagt, dass damals noch etwas galt und nicht Chaoten wie in der Hafenstraße von den Politikern und der Presse gehätschelt wurden.

Ganz unscheinbar sind sie zu zwei Bürgern geworden, die nur zufällig im Beruf Polizist sind. Sie wollen sich gerne überzeugen lassen, nur hat es ihnen bisher noch nie jemand so richtig erklärt. Vielleicht denkst du, sie sind ja auch vom Geld abhängig und ausgebeutet; wer weiß, wie viele da schon Dinge sagten, die sie gar nicht sagen wollten.

Als ich immer noch nichts sage, wie ein Klotz dasitze und aus dem Fenster starre, versuchen sie, an mein Ehrgefühl und an meine Aufrichtigkeit zu appellieren. Wenn ich etwas getan hätte, müsste ich doch dazu stehen „Ein Deutscher steht zu seiner Tat.“ Es handele sich ja um nichts Kriminelles, sondern um was Politisches.
Wie wolle man ein Beispiel geben, wenn man nicht zu seiner Tat stehe? Das würden sie respektieren, da hätte ja manch Krimineller mehr Ehrgefühl im Leibe. „Machen sie reinen Tisch. Sie wissen, die Gerichte werden es Ihnen zu Gute halten.“ So wären sie leider gezwungen, deinen ganzen Bekannten- und Freundeskreis zu überprüfen, die würdest du nun auch noch mit in die Sache reinziehen. Und immer offener und drohender werden sie, sie hätten eh schon genug Material, das reiche schon für ein paar Jährchen. Man könne dich hier in einer Ecke verschimmeln lassen, mit solchen wie dir werden sie schon lange fertig, und nicht alle Beamten wären so freundlich wie sie. Der „Väterliche“ schlägt plötzlich mit der Faust auf den Tisch und schreit, er habe jetzt genug von dir. Dann bringen sie mich nach unten in einen Gitterverschlag und lassen mich ein paar Stunden „schimmeln.“ Diese Stunden wollen kein Ende nehmen. Du willst dösen, kannst nicht, hin- und hergehen geht auch nicht. Und ständig gehen dir Fragen durch den Kopf. Worauf wollen sie heraus? Was haben sie mit mir vor? Schließlich kommen sie wieder. „Na, haben Sie sich es

überlegt, wollen Sie jetzt unsere Fragen beantworten?“ Ich will noch nicht: Aber jetzt haben auch sie genug. Sie lassen mich in Ruhe, und ich werde zurück ins Untersuchungsgefängnis gebracht. Diesmal erscheint mir meine Zelle fast wie ein Paradies.

Ein Weiteres Beispiel für die Taktik der Polizeibeamten:
Sie versuchen, die Beziehung zu Personen, die uns emotional nahe stehen, auszunutzen.

Wenn sie anders nicht mehr weiterkommen, greifen die Beamten zu dem Mittel, den zu Vernehmenden mit seinen Eltern, seinen Freunden, seinen Ehepartner, seinen Kindern oder anderen Personen zusammenzubringen. Sie gehen davon aus, dass es in unserer Verwandtschaft oder unter den Menschen, denen wir uns verbunden fühlen, jemanden gibt, der in der Lage ist, uns umzustimmen. Die Spekulation der Beamten ist folgende: Sie sehen, Zwang und Drohung, Überredung und Verängstigung helfen nicht. Sie haben auch keine Beamten, die in der Lage sind, zu dir eine emotionale Beziehung aufzubauen, so dass du dem Beamten zuliebe aussagen würdest. Also wählen sie unter Bezugspersonen Leute aus, denen zuliebe du einiges tun würdest, die du nicht enttäuschen willst, denen gegenüber du Anlass zu Respekt oder Dankbarkeit hast. Es müssen Personen sein, die politisch und juristisch nicht durchblicken, also nicht durchschauen, wofür sie benutzt werden sollen. Sie sollen die Doppelrolle des Lockvogels spielen:

Einerseits Deinesgleichen, mit dir befreundet oder verwandt, andererseits im Dienst derer, die dich kleinkriegen wollen. Und sie merken es nicht, weil sie oft einem anderen Denken und Wissen verhaftet sind. Die Frage, ob du aussagst oder nicht, soll zu einer Entscheidung zwischen dir und deinen Eltern, zur Existenzfrage deiner Beziehung zu ihnen hochgeschraubt werden.

Es gehört zu den größten Zynismen der Polizei, die Eltern eines Betroffenen zu benutzen, um ihn in die Knie zu zwingen. Jeder weiß, dass gerade die Eltern den Angstmechanismen noch viel mehr unterworfen sind als wir, die wenigsten einen relativ größeren Durchblick haben. Eure Eltern haben den Beamten gegenüber häufig überhaupt keine Widerstandskraft. Sie scheuen sich noch mehr als ihr dem freundlichen Beamten unfreundlich, also angemessen zu begegnen. Sie sind in ihrem Zweifel oft schnell genug bereit einzusehen, dass es für ihr Kind doch nicht gut sei, sich weiterhin zu weigern. Sie sind meist die geeignetsten Opfer für alle Drohungen und Schwarzmalerei der Beamten. Dann kommen sie zu dir in die Zelle. Es geht dir nicht gut. Sie sehen das und du siehst sie weinen, leiden und dich beschwören. Und du sagst kein Wort. Aber du hast Angst, sie ganz kaputt weggehen zu sehen. Du weißt nicht, wie du ihnen deine Lage begreiflich machen sollst. Du entwickelst Ihnen gegenüber Schuldgefühle. In dieser Situation darfst du nicht vergessen, dass deine Schuldgefühle die genau einkalkulierte fünfte Kolonne der Beamten sind. Die Schuldgefühle sollen in dir die Arbeit der Beamten leisten und dich zum Fallen bringen. Diese Situation gegenüber deiner Frau, deinem Mann oder Kindern ist noch viel schlimmer, weil sie zu der emotionalen Seite noch deine Verantwortung hinzufügen.

Zu ihnen darfst du ein Wort sagen: Sie sollen mit deinem Anwalt sprechen; der kann ihnen dann erklären, wie deine Situation aussieht. Aber nur mit deinem Anwalt. Verzichte auf jede Rechtfertigung und Diskussion!

Eine weitere Schwäche, auf die Beamten zählen, ist unsere Neigung, unser Tun überall und gegenüber jedem zu rechtfertigen. Vielen von uns ist es unerträglich, mit dem Gedanken herumzulaufen, etwas zu tun, dieses aber nicht zu rechtfertigen. Auch das mag in manchen Situationen des täglichen Lebens richtig sein. In der Situation der Vernehmung ist es absolut falsch. Es ist genauso falsch, auf die Idee zu kommen, den Beamten gegenüber jetzt zwar keine Aussage zu machen, ihnen aber haarklein darzulegen, dass man nur seine Rechte als Beschuldigter wahrnimmt.

Denk daran:
Kein Wort der Rechtfertigung. Überlege dir lieber, wer Anspruch auf Rechtfertigung hat: Nur wer dich auch kritisieren darf. Du wirst zugeben müssen, dass der Beamte hierzu nicht die Berechti-

gung hat. Auf irgendeine Art wird der Beamte immer wieder versuchen, mit dir ins Gespräch zu kommen. Er wird dich zum Beispiel bei deiner Intelligenz packen wollen, oder er wird versuchen, mit dir politisch zu diskutieren. Hierbei benutzt er Wissen, welches er sich im Laufe seiner Arbeit aneignen musste. Er hat sich sicher mit einigen politischen Schriften beschäftigt. Er wird versuchen, bei dir die Stellen herauszufinden, in denen du möglicherweise unsicher bist, in denen du politisch vielleicht verzweifelst. Er wird mit allen möglichen Zitaten aufwarten, um dir zu erklären, dass Ïhrppolitisch falsch liegt. Vielleicht trifft er genau die Position, die du selbst in Diskussionen mit deinen Kameraden erfolglos vertreten hast. (Er kennt sie vielleicht aus V-Material). Du meinst, bei ihm ëchtesÏnteresse zu spüren. Lass ihn sich abzappeln! Er hat mit dir nichts zu tun. Er macht die Sprünge schließlich nur, um dich zum Reden zu bringen. Wenn er wirklich politisches Interesse hätte, bräuchte er nicht warten, bis du antwortest.

Du hast es nicht nötig, den Beamten zu imponieren. Hüte dich davor, deinem Gegenüber in dieser Situation in irgendeiner Weise zu imponieren. Frag dich lieber, ob es nicht zu ertragen ist, längere Zeit mit einem Beamten zusammenzusein, ohne es ihm wenigstens einmal zu geben. Denk daran, dass deine Position nicht nur schwach, sondern auch stark ist.
Mach nicht den Fehler, dem Anderen zeigen zu wollen, dass du der Stärkere, der Klügere, der Gebildetere und politisch Bewusstere bist; denn dann bist du der Dumme. Er wird sofort darauf einsteigen und dir mit Interesse folgen und durch „dumme“ Zwischenfragen deinen Redefluss ankurbeln. In Wirklichkeit kannst du ihm nur dadurch imponieren, dass du in jeder Situation bei deinem Schweigen bleibst.

3 Datenschutz - Sicherheit 2.0

Einleitung:

Weshalb Datenspuren vermeiden sowie Kommunikation und Daten verschlüsseln? Informationstechnologie ist in den Alltag eingekehrt, wird auch weiterhin günstiger, leistungsfähiger, kleiner, leichter, mobiler und bald beinahe allgegenwärtig sein.

Obwohl Datenschützer seit langem warnen sind vielen Menschen erst mit dem Bekanntwerden der Bespitzelung und Ausforschung von Journalisten und Gewerkschaftern durch die Telekom und andere Unternehmen zumindest einige der vielfältigen Möglichkeiten des Missbrauchs von alltäglich erhobenen und gespeicherten Daten bewusst geworden.

Das Missbrauchspotenzial dieser Daten reicht vom Anlegen von Bewegungsprofilen bis hin zur Ausforschung von sozialen und beruflichen Netzwerken und Kontakten, beruflichen und privaten Aktivitäten sowie der kompletten Telekommunikation. Denn wegen immer leistungsfähigerer und günstigerer Informationstechnik, Infrastruktur, Software und Speichermöglichkeiten in früher kaum vorstellbarer Größe stellt eine massenhafte und langfristige Erfassung und Speicherung umfangreicher personenbezogener Informationen rein technisch und ökonomisch betrachtet keinen unverhältnismäßigen Aufwand mehr dar. So sind automatisches Speichern aller greifbaren Informationen und das Errechnen sehr umfangreicher Personenprofile gängige Praxis geworden. Trotz Millionen und Milliarden von Datensätzen erfordert auch eine Auswertung und Nutzung der massenhaft gespeicherten Daten bzw. das Filtern der vielen Informationen nach bestimmten Personen, Nummern, Adressen und anderen Kriterien mit aktueller Informationstechnik nur relativ geringen Aufwand.

Trotzdem findet digitale Kommunikation über nicht vertrauenswürdige Kanäle wie Internet weiterhin immer noch viel zu oft völlig ungeschützt statt und ist damit sehr leicht auch für Unbefugte zugänglich. Zudem werden beim Arbeiten mit moderner Standard-Informationstechnik ständig Daten im Hintergrund generiert, gespeichert und versendet. Davon haben die Wenigsten überhaupt Kenntnis und schützen sich folglich auch nicht vor Missbrauch dieser unbewusst angelegten

Metadaten.

Auch Computer oder Notebooks inkl. Festplatte oder Datenträger wie z.B. USB-Sticks oder externe Festplatten sind heutzutage verbreiteter, kleiner, leichter und mobiler und dadurch einfacher verloren oder entwendet, wobei wegen der Menge sowie Relevanz der dort gespeicherten Daten deren Wert oft den der Technik übersteigt und diese nicht selten das eigentliche Ziel von Diebstählen sind.

Auch illegale Durchsuchungen und Beschlagnahmungen von Datenträgern durch Behörden z.B. wegen unbequemer Berichterstattung oder unliebsamer politischer Betätigung kommen immer wieder vor. Hinzu kommen die zunehmende Überwachung durch Behörden und Geheimdienste und die von diesen zudem nutzbaren Datenberge inklusive umfangreicher Personenprofile durch die Erhebung, Speicherung und Auswertung von Daten und Kommunikation zu kommerziellen Zwecken.

Zahlreiche Beispiele zur illegalen Erhebung und dem Missbrauch von Daten liefern sowohl Unternehmen, Kriminelle wie auch Behörden. Wer wirklich sicher gehen möchte oder muss, sollte sich nicht auf Grundrechte ignorierende Regierungen, Behörden, Geheimdienste und Datenschutzgesetze ignorierende Wirtschaft verlassen, sondern sich selbst um technischen Datenschutz kümmern. Denn nur Daten, die durch bewusstes Verhalten nicht vorhanden oder durch Verschlüsselung nicht zugänglich sind, können nicht missbraucht werden. Also sollten Datenspuren vermieden werden und auf Datenträgern enthaltene oder über das Internet oder Funknetzwerke verschickte Daten vor Unbefugten geschützt, also verschlüsselt werden.

Dabei dürfen mögliche Fallen und Tücken nicht ignoriert werden. Denn gefährlicher als gar keine Sicherheit kann trügerische Sicherheit sein.

So kann Verschlüsselung z.B. wegen naiv gewählten Passwörtern beinahe wirklungslos sein.

Wer extrem senible Daten speichert, muss zudem wissen:
Mit genügend Aufwand und Fachwissen kann beinahe jeder Verschlüsselungsschutz ausgehebelt oder umgangen werden.

Wegen meist recht aufwendiger und damit auch recht unwahrscheinlicher Möglichkeiten des Aushebelns von Schutzmechanismen auf diese zu verzichten, wäre jedoch purer Leichtsinn und ähnelte einem Absprung ohne Fallschirm, weil dieser ja auch versagen oder manipuliert werden kann.

3.1 Datenschutz

Das Weltnetz wird in Zeiten von Web 2.0 geradezu von Angeboten überflutet, welche möglichst viele Daten in den Datenbankprofilen sammeln möchten. Die etwas älteren werden sich noch an das Aufkommen der Mailboxen Mitte der 80er oder den rasanten Anstieg an Netzforen erinnern.

Heutzutage wird der Nutzer jedoch mit Möglichkeiten überflutet, die vor Jahren noch als reine Utopie abgestempelt worden wären. Da kann man zum Beispiel auf YouTube Videos jeder Art zügig hochladen und verbreiten, kann per MySpace, Facebook, Wer-Kennt-Wen oder den vielen VZs Teil eines sozialen Netzwerkes mit eigenem Profil werden oder einfach ein öffentliches Tagebuch, hier Blog genannt, führen welches für jede zugänglich ist.

Neben so manchen Annehmlichkeiten, die wir durch genannte Dienstleistungen, besonders in Hinsicht der Verbreitung von Propaganda und volksaufklärenden Inhalten, erfahren, bergen sich dennoch ebenso viele Gefahren dahinter. Für Datensammler, welche im Auftrag der Regierung Profile von uns erstellen sollen, sind solche selbstangelegten Profile natürlich ein gefundenes Fressen. Über

MySpace finden sie heraus in welcher Region wir wohnen, per YouTube können sie uns auf Videoaufnahmen erkennen und dadurch wissen wo wir zugegen sind und per Facebook unserem Profil in der Akte dazu noch ein Bild verpassen. Dieses Profil wird ständig mit Informationen gefüllt, die wir unachtsam im Netz hinterlassen. Entweder diskutieren wir über Lieblingsfilme, Lieblingsgerichte, Lieblingsautomarken oder gar über konkrete Dinge wie unser Auto, unser Haarschnitt, Klamotten, Erkennungsmerkmale, Freunde und so weiter.

Deshalb geben wir dir folgende Hinweise, die dazu beitragen, es den Schnüfflern so schwer wie möglich zu machen:

Nutze bei Profilen, die du im Netz anlegst, stets eine eBrief-Adresse bei einem Anbieter, der keine Personenbezogene Daten von dir hinterlegt hat.

Nutze bei der Wahl des ePostfach-Anbieter keine deutschen, da diese der TKÜV (Telekommunikations-Überwachungsverordnung) unterliegen und dich somit überwachen müssen bzw. Einsicht in deinen Nachrichtenverkehr haben und diesen auch an staatliche Behörden weitergeben können.

Gebe bei deinen Profilen und Nachrichten, die du im Netz hinterlässt, keine personenbezogenen Daten von dir ein.

Hüte dich davor Dateien zu verbreiten, die Rückschlüsse auf deine Person zulassen (z.B. Fotos) die dich zeigen oder Textdokumente in welchen als Autor dein Name steht.

Sei insgesamt vorsichtig, wenn es darum geht, Angaben über die eigene Person zu machen oder wenn du über private Dinge befragt wirst. Im Netz kannst du dir nicht sicher sein, dass der Gegenüber auch wirklich der ist, für den er sich ausgibt. Misstraut unseriösen Angeboten und meidet soziale Netzwerke. Außerdem raten wir tunlichst davon ab, sogenannte Filesharing-Programme wie zum Beispiel eMule zu nutzen. Durch solche erhälst du schneller eine Anzeige aufgrund Urheberrechtsverletzungen als dir lieb ist.

3.2 Das Passwort

Passwortgeschützte Daten sind nur dann sicher, wenn auch das Passwort, mit denen sie verschlüsselt wurden, sicher ist. Der sicherste Verschlüsselungsalgorithmus nützt wenig, wenn als Schlüssel ein einfach zu erratendes Passwort verwendet wird.

Dabei meint „einfach zu erraten“ nicht nur Personen, die z.B. die Namen deiner (Ex-)Partnerin, Freundin, Haustiere, Kinder oder Lieblingsbands sowie Wörter zu deinen Hobbies oder aus deinen Interessens- und Arbeitsgebieten ausprobieren, um an deine Daten zu kommen.

3.3 Gefahren für dein Passwort

Der Keylogger

Ein Keylogger ist eine Hard- oder Software, die dazu verwendet wird, die Eingaben des Benutzers an einem Computer mitzuprotokollieren und dadurch zu überwachen oder zu rekonstruieren. Keylogger werden beispielsweise von Hackern verwendet, um an vertrauliche Daten - etwa Kennwörter oder PIN - zu gelangen. Ein Keylogger kann dazu sämtliche Eingaben aufzeichnen oder gezielt auf Schlüsselwörter wie z. B. Passwörter warten und dann erst aufzeichnen, um Speicherplatz zu sparen.
Hier hilft dann auch nicht mehr das sichereste Passwort.

Die Phishing Attacke

Die zweite Möglichkeit besteht darin, das Opfer zu „Verarschen“. Im großen Stil funktioniert das über Phishing. Hier werden dem Nutzer auf eine gemeine Weise die Zugangsdaten geklaut.

Ein kleines Beispiel für die Verständlichkeit:

Ich möchte mich bei Amazon einloggen. Gebe also oben in der Webadresse www.amazon.de ein. In wirklichkeit habe ich aber ein Tippfehler begangen, und habe www.aamazon.de eingegeben. Doch mir fällt nichts auf weil die Seite genauso aussieht, wie die echte. Logge mich also ein und werde zur richtigen amazon Seite umgeleitet als wäre nichts geschehen. In Wirklichkeit hat die gefälschte Seite im Hintergrund meine eBrief-Adresse und Passwort in eine Datenbank gespeichert, die dem Angreifer zur verfügung steht.

Die Holz Hacker Methode

Kommen wir nun zu einer Methode, die gerne eingesetzt wird um einzelne Konten gezielt zu knacken. Die eingesetzte Methode heißt: Bruteforce. Sogenannte Bruteforce Programme probieren jede Möglichkeit aus, bis Sie das richtige Passwort erraten haben. Je mehr Möglichkeiten, desto länger benötigt das Programm.

Über mehr Rechenleistung bei modernen Prozessoren und Grafikkarten freuen sich nicht nur der Computer-Anwender, sondern auch die Passwort-Knacker. Je leistungsfähiger die Rechner sind, desto schneller haben sie ein Passwort durch simples Ausprobieren aller möglicher Zeichenkombinationen gefunden.

Forscher der Firma Electric Alchemy haben die Kosten fürs Knacken einer mit 9 Zeichen verschlüsselten ZIP-Datei per Brute-Force berechnet: Bei EC2 sind für solch ein Passwort, das nur aus Buchstaben und Zahlen besteht, weniger als 2000 Dollar und eine Stunde Zeit nötig.

Zugegeben: 2000 Dollar sind kein Schnäppchenpreis. Und die Kosten steigen bei längeren Passwörtern dramatisch an. Doch Hacker haben noch ganz andere Mittel, um an ein Passwort zu kommen.

Server-Hacks

Selbst das längste Passwort schützt dich nicht, wenn Hacker es im Klartext von einem Server klauen können. Das ist in den vergangenen zwei Jahren mit Millionen Passwörtern geschehen. Etwa bei Yahoo, wo die Diebe eBrief-Adressen und Klartext-Passwörter von mehr als 450 000 Nutzern stehlen konnten. Die Daten veröffentlichten sie anschließend im Weltnetz.

Erschreckend ist alleine, wie häufig es Hacker schaffen, an die Datenbanken großer Internet-Firmen zu gelangen. Dass diese Firmen, wie im Falle von Yahoo, die Passwörter im Klartext gespeichert haben, ist eine Schande für die Firma und eine Katastrophe für die Nutzer. Computer-Hacks

Bei den Passwort-Dieben ist der Server-Einbruch ebenso beliebt, wie der Einbruch auf dem Computer des Heimnutzers. Diesen erledigen aktuelle Viren, etwa Keylogger und Browser-Passwort-Trojaner für ihn. Zumindest gegen diese Angriffe kann sich der Anwender mit einem Antiviren-Programm und gebotener Vorsicht beim Laden von Dateien halbwegs gut schützen.

Die „Passwort vergessen“ Option

Sollte ein Hacker mit keiner der bisher genannten Methoden an dein Passwort gekommen sein, dann kann er die Passwort-Zurücksetzfunktion von Webdiensten nutzen. Damit die Funktion wirkt, muss man eine Sicherheitsabfrage beantworten können, etwa: „Wie lautet der Geburtsort deiner Mutter?“.
Ist das geschehen, erlischt das aktuelle Passwort umgehend und man darf ein neues Passwort

vergeben. Das große Problem an dieser Methode: Die nötigen Infos sind meist nicht besonders geheim. In der Regel besitzen diese Infos schon die meisten Freunde, Bekannte, oft aber auch Kollegen oder bei Kindern die Mitschüler. Führt einer von ihnen Böses im Schilde, kann er sich so spielend in viele Internetdienste hacken. Echte Hacker kommen an die nötigen Funktionen über eine Recherche im Internet und die Suche in sozialen Netzen.

3.4 Passwortwahl

Die Frage, die sich einem stellen sollte, wenn man sich ein neues Passwort zulegen muss, sollte stets sein: Wie kann ich es lang genug machen, mir es aber trotzdem einfach merken können?

Ein sicheres Passwort erkennt man an den folgenden Aspekten:

- Es beinhaltet mindestens(!) 8 Zeichen
- Es beinhaltet große und kleine Buchstaben (a-z, A-Z)
- Es beinhaltet Zahlen (0-9)
- Es beinhaltet Sonderzeichen („_“, „+“, „?“, „#“, „&“, „%“)

Befolgst du nun diese 4 Regeln entstehen z.B. Passwörter wie „j7%_P+1r&U“, „e56U_W?a0“ und so weiter. Zugegebenermaßen sind solche wirren Zeichenfolgen für den Ungeübten ziemlich schlecht zu merken. Deshalb geben wir weiterführend den Rat: Baue dir deine Passwörter aus Sätzen!

Dadurch sind sie nicht nur einfacher zu merken, sondern gewinnen ebenfalls erheblich an Größe. Folgend nun zwei Beispiele:

Nachbar Müllers Hund heißt Bodo - **„0NACHbar1-2MuElLeRs?hund-8-hEiSsT-8-boDO“**

Susi hat lange blonde Haare - „sUSi-123-HAT-lANGebl0nde&H44Re“

Solche Passwörter sind sehr sicher und ebenso einfach zu merken, oder? Nach mehrmaligem Probetippen hat man sie sicher drauf. Du siehst außerdem, dass wir an der einen oder anderen Stelle Zahlen anstatt Buchstaben genutzt haben. Diese Schreibvariation (auch Leet-Speak genannt) bietet die Möglichkeit, ähnlich aussehende Zahlen und Zeichen einfach anstatt den ursprünglichen Buchstaben zu nutzen. Hier eine kleine Liste:
A = 4
B = 8
C = (
D =)
E = 3
G = 9
H = -
I = 1
O = 0
R = 2
S = 5

Neben diesen Vorschlägen kannst du natürlich auch eigene Kreationen nutzen. Es ist alles Recht, sei es noch so komisch, es dient letztendlich deiner Sicherheit.

Es gibt wage Schätzungen wie lange ein Supercomputer für das Knacken eines solch langen Passwortes brauchen würde. Diese sind aber definitiv nicht aussagefähig, da die Technologie voranschreitet und damit die Verarbeitungsgeschwindigkeit eines Rechenprozessors stets zunimmt.

Nehmen wir mal an, man hält sich an die o.g. Regeln, und nutzt alle Zeichenkategorien aus dem ASCII-Zeichensatz. Demnach gäbe es 93 verschiedene Zeichen die man verwendet haben könnte (33:! bis 126: ~). Der Angreifer weiß nicht genau welche, und muss deswegen von allen ausgehen. Die Anzahl der möglichen Kombinationen ergibt sich aus:

Anzahl = Zeichenanzahl ^Passwortlänge.

Bei unserem Beispiel mit einer Passwortlänge von 8 Zeichen entspricht das:

Anzahl = 93 hoch 8
Anzahl = 5.595.818.096.650.401 Möglichkeiten

Wenn der Angreifer es schafft, 1.000.000 Passwörter pro Sekunde zu testen, was bei einem Login auf ein Forum utopisch sein dürfte, dann würde die Person immer noch 5595818096 Sekunden brauchen, was rund 177 Jahren entspricht. Wir raten dir: Besser ein Zeichen zu viel als zu wenig!

Wenn sich der Staat auch überlegt für das Knacken deines Passwortes solch einen Supercomputer für 5-6-stellige Euro-Summen zu beauftragen, steht es nicht mehr in unserer Macht dies zu verhindern, haben wir aber alles Mögliche getan, unser Passwort so sicher wie möglich zu gestalten und es der Maschine so schwer wie nur möglich zu machen.

Deine persönlichen Passwörter sind die Schlüssel zu deinen Informationen. Gehe also sehr vorsichtig mit ihnen um und notiere sie dir nirgends, deinen Haustürschlüssel würdest du in der Öffentlichkeit auch nicht überall hinlegen, oder? Ebenso wenig solltest du ungeschützte Passwortlisten auf dem Rechner erstellen oder diese im Mobiltelefon speichern.

Falls du dennoch zu viele Passwörter besitzt um sie dir merken zu können, dann nutze z.B. Programme wie KeePass um sie sicher zu verwalten.

Desweiteren legen wir dir folgenden Rat ans Herzen:
Um die Sicherheit deines Passwortes stets zu gewährleisten, solltest du es regelmäßig, im Idealfall alle 6-9 Monate, ändern. Dies schützt dich davor, dass Dritte dein Passwort eventuell erfasst haben und es ohne deine Kenntnis ab und zu selbst nutzen.

Geheimhaltung des eigenen Passwortes:

Das sicherste Passwort ist nicht mehr sicher wenn man es jedem weitergibt dem man vertraut. Ein Passwort sollte man immer nur für sich behalten. Auch dem Lebens- oder Ehepartner sollte man ein Passwort niemals mitteilen. Man kann jetzt sagen, dass es ein Vertrauensbruch darstellt aber auch unbeabsichtigt kann dadurch das sicherste Passwort an die falschen Leute geraten. Zum Beispiel wenn das Passwort leichtsinnig auf der Arbeit unter Beobachtung eingegeben oder sogar aufgeschrieben wird. Gerade aber aufschreiben oder in eine Textdatei speichern sollte man ein Passwort nicht.

Dies ist nur eine Anregung zur Zusammenstellung eines Passworts. Der Fantasie sind dabei eigentlich keine Grenzen gesetzt. Das Gegenteil ist der Fall. Wenn man sich eine eigene Methode zur Erstellung eines Passwortes einfallen lässt ist es sogar noch individueller und damit auch sicherer.

3.5 Passwort-Generator

Warnung vor Passwortgeneratoren im Weltnetz

Mir fallen in letzter Zeit immer wieder Weltnetzseiten auf, die Passwortgeneratoren anbieten, welche in der Eingabemaske den Namen der Weltnetzseite oder eine eBrief-Adresse abfragen, die mit dem Passwort geschützt werden sollen.

Ohne das speziell untersucht zu haben, ist hoffentlich von selbst klar, dass man diese „Hilfsmittel" auf keinen Fall nutzen sollte. Man würde einer unbekannten Person sowohl seine Weltnetzseite / eBrief-Adresse als auch mutmaßliches Passwort übergeben - freiwillig! Ein Passwort-Generator im Weltnetz ist wirklich nur dann sinnvoll, wenn der Generator(-Betreiber) nicht weiß & nicht wissen kann, wer das Passwort für welchen Zweck hat generieren lassen.

3.6 Aufbewahrung von Passwörtern

Ein Passwortmanager besteht meist aus ein bis drei Teilen:

- Ein Hauptprogramm für deinen Computer, das die Zugangsdaten (Welche Weltnetzseite? Welcher Nutzername? Welches Passwort?) in einer (mit Passwort verschlüsselten) Datenbank verwaltet und verschiedene Zusatzfunktionen bietet.
- Ein Plug-In für die Netzbetrachter, dass diese Zugangsdaten dann (halb)automatisch einträgt, wenn man das abruft. Das ist optional, man könnte das auch von Hand übernehmen.
- Ein (irgendwie synchronisierbares) Gegenstück auf Android, iPhone/iPad (iOS) und anderen Smartphone-/Tablet-Mobilsystemen, mit dem man mindestens die Passwortdatenbank laden, öffnen und anzeigen kann, zuweilen auch bearbeiten.

Damit die Passwörter im Passwortmanager sicher sind, rückt er diese nur auf Anfrage heraus - und nur nach Angabe einer Art „Masterpasswort". Dieses Passwort sollte natürlich etwas sicherer sein als üblich, weil es ja alle anderen Passwörter schützt und daher nicht weniger sicher sein darf als diese. Gründe für Passwort-Manager

Es gibt viele Gründe für einen Passwortmanager:
Keine Kennwörter mehr merken.

Weil alle im Passwortmanager gespeichert sind. In der Realität sollten Sie sich einige wichtige dennoch merken und nicht im Passwortmanager speichern.
Bessere Passwörter!

Weil wir uns keine Passwörter mehr merken müssen, können wir diese wahnsinnig übertrieben kompliziert machen - ohne daran zu verzweifeln!
Komplexere Passwörter!

...denn viele Passwortmanager enthalten auch gleich einen Passwort-Generator! Der hält uns davon ab, „katze67" zu verwenden, nur weil uns nichts besseres einfällt.
Überall andere Passwörter!

Weil wir uns keine Passwörter mehr merken müssen, sind wir nicht mehr in Versuchung, bei allen Diensten nur ein gemeinsames Passwort zu haben. Du kannst bei jedem Dienst ein anderes Passwörter haben, musst dir aber trotzdem nur ein Kennwort merken - nämlich das Passwort des Passwort-Managers.

Ständig andere Passwörter!

Weil wir uns keine Passwörter mehr merken müssen, können wir öfter mal ein Passwort ändern, wir müssen uns ja weder das neue merken noch das alte vergessen.
Weniger Phishing!

Passwortmanager speichern ein Passwort für eine bestimmte Weltnetzseite und geben es nur dort automatisch an. Das bedeutet, dass wenn du ein Zugangsdatenfeld vor dir hast, und der Passwortmanager sich weigert, es auszufüllen, dann bist du vielleicht auf der falschen Seite! Andersherum: Einige Passwortmanager rufen z.B. per Doppelklick die gewünschte Seite auf und geben dann direkt Name und Passwort ein - so ist man sicher, sich wirklich dort anzumelden, wo man sich anmelden will.
Mehr Komfort!

Passwortmanager können, je nach Ausführung, automatisch anzeigen, ob die gewählten Passwörter sicher sind; sie können nach Ablauf einstellbarer Zeit darauf hinweisen, dass ein Passwort gewechselt werden sollte; sie können Notizen zu Passwörtern speichern, teils auch Dateien; einige bieten auch spezielle Bereiche an, etwa um auch Software-Keys zu verwalten.

Kurzum:

Mit einem Passwortmanager ist es leichter, sicherer mit Passwörtern im Weltnetz umzugehen.

Meine paranoiden Sicherheitstipps zu Passwort-Managern
Superduperlanges Passwort-Manager-Zugangs-Kennwort!

Wenn alle Passwörter im Passwortmanager liegen, dann sind sie darin nur so sicher wie das Passwort, mit dem du deine Passwortdatenbank gesichert hast. Daher sollte das wirklich lang und kompliziert sein.
Keine Cloud, kein Sync nutzen!

Natürlich verbietet es sich von selbst, die Datenbankdatei in Cloud-Speicher zu stellen oder über sonstige Cloud-Dienste zu nutzen. (Viele Produkte bieten das an, aber man kann die Passwort-Datenbankdatei auch manuell verschieben.
Vorsicht vor der Zwischenablage!

Das Funktionsprinzip vieler Passwortmanager ist, die Zwischenablage zu verwenden, um Passwörter zur Verfügung stellen. Das bedeutet auch: Wenn dein System kompromittiert ist, durch Virus/Malware/Trojaner/Keylogger, dann besteht die prinzipielle Gefahr, dass über das Auslesen der Zwischenablage Passwörter ausspioniert werden. Das gilt auch für Mobilgeräte. Es gilt wie stets: Auf einem unsicheren System kann keine Software sicher sein.
System verschlüsseln!

Um deine Passwort-Datenbank-Datei vor unbefugtem Zugang zu schützen, sollte der Rechner, also die Systempartition verschlüsselt sein, bei Tablets und Smartphones natürlich das jeweilige Gerät (iOS ab Werk; Android: Android verschlüsseln). So könnte ein Angreifer nur schwer einen Software-Keylogger/Trojaner heimlich aufspielen, etwa in deiner Abwesenheit vom Rechner. Gegen einen Hardware-Keylogger würde dies natürlich nichts ausrichten, hierfür bieten Passwortmanager aber virtuelle Keyboards.
Sicherheitsstufen einführen!

Natürlich speichere um Himmels willen nicht alle deine Passwörter im Passwortmanager! Statt dessen lädst du darin nur den ganzen unwichtigen Ballast ab, irgendwelche Foren, in denen es um

nichts wichtiges geht, das siebzehnte soziale Netzwerk, das eh keiner nutzt, etc.

Eine Handvoll von Passwörtern solltest du dur weiterhin merken und sie auf keinen Fall im Passwortmanager speichern, also zum Beispiel TrueCrypt Passwörter, PayPal, Online-Banking. Stelle dir sozusagen Sicherheitsbereiche und Hochsicherheitsbereiche vor: Sicherheitsbereiche haben Passwörter, die du im Passwortmanager speicherst; Hochsicherheitsbereiche haben Passwörter, die du NIRGENDWO speicherst, außer im Kopf. Das ist unbequemer, aber sicherer.

3.7 KeePass Password Safe

Bei solch einfallsreichen und langen Passwörtern stellt sich uns ein weiteres Problem in die Quere:

Wenn man für jeden Anbieter, bei dem man ein Passwort benötigt, ein anderes, 20-Zeichen langes, Passwort mit Zahlen und Sonderzeichen nutzt, wie soll man sich diese dann bitteschön alle merken?

Der ein oder andere mag zwar ein Gedächtnisgenie sein und somit keine Probleme damit haben, der Großteil aber würde sich diese auf einem Stück Papier oder gar auf dem Rechner notieren. Um diesem erheblichen Sicherheitsrisiko entgegenzuwirken, gibt es ein Programm namens KeePass Password Safe.

Dieses Programm legt eine, mit den Algorithmen AES und Twofish, vollverschlüsselte Datenbank an in der die verschiedenen Passwörter mit dem dazugehörigen Anbieter als Datensätze angelegt werden. Man muss sich somit nur noch das Haupt-Passwort für den Zugang zu dem Programm merken. Dieses sollte natürlich besonders sicher sein und mit viel Bedacht gewählt werden, ebenfalls regelmäßig gewechselt werden.

Für dein Android Mobiltelefon gibt es die Erweiterung (App) KeePassDroid um deine Passwörter sicher zu Speichern. Beim ersten Start kannst du in der App eine neue Passwortdatenbank anlegen oder eine bereits bestehende Datenbank öffnen - ideal, wenn du bereits zuvor am Computer eine Passwortdatenbank erstellt hast.

Hier gezeigte Programmversion: Professional Edition - 2.20.1

Zuerst lädst du dir die neuste Version von KeePass Password Safe sowie die deutsche Sprachdatei herunter.

Du öffnest nun die Installationsdatei, wählst die Sprache Deutsch und bestätigst.

Nachdem du einmal Weiter gedrückt hast akzeptierst du die Lizenzvereinbarung und drückst weitere 3 mal auf Weiter.

Da du das Programm leicht wiederfinden möchtest machst du ein Häckchen in das Feld Desktop-Symbol erstellen. Weiter gehts mit Weiter.

Als nächstes wird auf Installieren gedrückt und das Programm kopiert sich auf die Festplatte.

Noch auf Fertig stellen drückt und die Installation wird abgeschlossen.

Nun öffnst du die ebenfalls zuvor heruntergeladene Sprachdatei und kopierst die Datei German.lngx in das Verzeichnis in welches du auch das Programm installiert hast, üblicherweise C:/Programme/KeePass Password Safe 2.

Nachdem du das Programm gestartet hast, drückst du oben auf View ¿ Change Language, dort wählst du die Sprache Deutsch aus und bestätigst mit Ja. Das Programm startet nun selbstständig neu.

Im Hauptfenster wählst du nun oben Datei ¿ Neu und erstellst mit einem sicheren Passwort eine Datenbank.

Ist diese erstellt, erscheint links eine Verzeichnisstruktur anhand welcher du deine einzelnen Passwörter kategorisiert sichern kannst.

Die beiden Standart Punkte im rechten Fenster kannst du ohne bedenken löschen.

Suche dir nun in der linken Verzeichnissruktur den Punkt aus in dem du das Passwort gerne speichern möchtest und gehe dann auf Bearbeiten und Eintrag hinzufügen

Im folgenden Fenster kannst du nun den Titel des Eintrags, den Benutzernamen sowie das dazugehörige Passwort und eventuell einen Kommentar dazu eingeben. Es ist auch definitiv empfehlenswert, dem Passwort ein Verfallsdatum zu geben, damit man automatisch regelmäßig seine Passwörter ändert. Dadurch kann man sicherstellen, dass von einem Dritten notierte Passwörter ungültig gemacht werden.

Nachdem du die Felder ausgefüllt hast, bestätige mit OK und ein neuer Eintrag erscheint nun in deiner Datenbank. Diese Vorgehensweise wiederholst du nun mit all deinen Passwörtern, welche du in der Datenbank speichern möchtest.

Wichtig ist nur, ein sicheres Haupt-Passwort zu wählen, welches du auch nicht so schnell vergisst, ansonsten wären ja auch deine ganzen anderen Passwörter weg. Die Datenbank wird beim Schließen des Programms automatisch wieder verschlüsselt und kann somit bedenkenlos auf der Festplatte oder anderen mobilen Datenträgern gesichert werden.

3.8 Schlüsseldateien - Besser als jedes Passwort

Alle Welt redet immer von sicheren Passwörtern, aber auch das sicherste Passwort des Planeten kann noch verbessert werden - durch eine Schlüsseldatei. Eine solche Datei wird beim Login zusätzlich zum Passwort verlangt und kann jede beliebige Datei sein, einige Tools akzeptieren sogar ganze Programmsammlungen.

Selbst wenn ein Angreifer dein ünsicheresPPasswort aufdeckt, müsste er immer noch den richtigen Datenträger mit der richtigen Datei als Schlüssel finden. Lasse mal die Dateien auf deinem Windows-System zählen und überlege selbst, ob er wohl Erfolg hat.

Programme bei denen du derlei Schlüsseldateien einsetzen kannst, sind etwa der Passwort-Save KeePass sowie die Verschlüsselungslösung VeraCrypt.

3.9 Die Schlüsseldatei

Die Schlüsseldatei ist eine Alternative zur manuellen Eingabe eines Kennworts. Damit können deutlich längere und komplexere Schlüssel verwendet werden und es besteht nicht mehr die Gefahr, das Kennwort zu vergessen. Allerdings kann die Schlüsseldatei durch Datenverlust verlorengehen. Das Angriffsszenario bei einem Kennwort besteht aus Ausspähen (beispielsweise durch einen Keylogger) oder Erraten (beispielsweise durch einen Wörterbuchangriff); eine Schlüsseldatei ist dagegen vor unbefugtem Zugriff zu schützen, damit sie nicht kopiert wird. Häufig werden

Schlüsseldateien deshalb zusätzlich mit einem Masterpasswort verschlüsselt.

4 Datenkraken

Die Firma Google weiß und protokolliert beispielsweise nicht nur, nach was du direkt auf der Google-Weltnetzseite wann gesucht und welche Ergebnisse du dann auch tatsächlich angesteuert oder was du dir wann wie oft auf Googles Videoplattform YouTube angeschaut hast.

Sobald Dienste wie z.B. Karten aus Google-Maps oder Videos aus YouTube in eine Seite eingebettet sind, werden diese direkt von Google geladen und Google damit - diesmal für die Besucher unbewusst - informiert, dass und wann du diese Seite abgerufen hast. Das gilt umso mehr, wenn beispielsweise ein von den Besuchern gar nicht wahrgenommener Dienst wie Google-Analytics zur Erstellung von Statistiken genutzt wird. Auch hier landen Informationen über alle Seitenabrufe auch bei Google.
Google Analytics

Was Google uns (und damit auch sich selbst) an Informationen liefert, ist extrem umfangreich. Google Analytics erhebt folgende Informationen:

- Herkunft der Surfer (Staat und Stadt bzw. Region)
- welche Sprache ist voreingestellt? Deutsch? Englisch?
- Betriebssystem (Linux Distribution, Windows, Mac OS X) oder Firmware vom Tablet-PC bzw. Smartphone
- welches Gerät kommt zur Anwendung?
- Browser mit Versionsnummer (Google Chrome? Firefox? Safari?)
- welche Add-ons werden in welcher Version verwendet? (Beispiel: Shockwave Flash, Java, JavaScript, Silverlight, Quicktime, Google Talk Plug-in etc.)
- Auflösung des Bildschirms (Anzahl Pixel Breite und Höhe)
- wie lange wurden die Artikel durchschnittlich gelesen? Haben sich die Surfer für einen ausführlichen Beitrag genug Zeit genommen?
- Besucherquellen: Suchmaschinen oder soziale Netzwerke (Facebook, Twitter), verweisende Webseiten?
- ging der Besucher innerhalb der Webseite woanders hin? Wenn ja, wohin? Oder wurde die Seite komplett verlassen?
- welche Dateien wurden heruntergeladen?
- welche Videos wurden angeschaut?
- kam der Besucher wieder oder besuchte er die Seite nur einmalig? (Feststellung per Cookie)
- wurden Werbebanner angeklickt?
- wurden Produkte verkauft?
- u.v.m.

Noch problematischer, da de facto Standard, ist die technisch ähnlich funktionierende über Google-Ads oder dem mittlerweile von Google aufgekauften Unternehmen DoubleClick eingebundene Werbung. Auch diese wird immer direkt von den Google-Servern geladen und der Datenkrake damit über die eigentlichen Seitenabrufe informiert.

Um dich dabei dauerhaft verfolgen und eindeutig identifizieren zu können, vergibt Google dazu eine dir zugeordnete Nummer, die im Hintergrund in einem sogenannten Cookie auf deinem Computer gespeichert und bei jedem der weiteren Abrufe wieder an Google übertragen wird.

Dabei reicht ein einziger Login, die Angabe von persönlichen Daten oder die beim Zugangsprovider gespeicherte Zuordnung der genutzten IP-Adresse zum Kunden, um ab dem Moment ein bereits jahrelang gepflegtes Profil einer konkreten Person zuordnen zu können.

Somit weiß und speichert Google eben nicht „nur“, was du mit dem Google Suchdienst wann gesucht und welche der Ergebnisse du dabei angesteuert hast, sondern erfährt meist auch sehr genau, wo du dich sonst noch herumgetrieben und was du dabei gelesen hast. Nutzt du zudem noch die Google-Toolbar oder den Webbrowser Google Chrome, wird auch noch der bisher nicht erfasste Rest ausgeleuchtet.

Dass sich Google auch über weitere persönliche Daten, wie z.B. deine Termine im Onlinekalender, über deine Notizen im Onlinenotizbuch oder bei Google Mail über den vollständigen Zugriff auf deine eBriefe (was schreibst du wann wem und wie oft und wer schreibt dir wann was und wie oft) freut, die es Ihrem Profil sowie bei eBrief auch dem Profil der an dich Schreibenden und/oder von dir Angeschriebenen - auch wenn diese selbst keine Google Dienste nutzen - zuordnen kann, sollte nicht mehr verwundern.

Trotzdem ist Google nicht das Problem an sich, sondern eher Symptom und als momentaner weltweiter Marktführer prominentestes Beispiel.

Wer örtlich näher liegende Beispiele sucht, kann sich die analoge Konzentration solcher Daten beim deutschen Marktführer United Internet bewusst machen: Diesem Konzern gehören Tochterunternehmen und breit genutzte Dienste wie z.B. 1&1, web.de und gmx, über die ein Großteil der deutschsprachigen Internetnutzung abgewickelt wird. Auch bei Ebay (Nutzungszeiten, Umsätze, Konsumverhalten, Interessen), Amazon (wer hat wann welche Bücher angeschaut oder bestellt), StudiVZ (Persönliche Daten, Themen, Interessen und vor allem soziale Netzwerke zukünftiger Eliten), Facebook (Soziale Netzwerke und Kontakte), MySpace (Interessen, wer kennt wen) und anderen marktführenden Plattformen kommen naturgemäß mit der Zeit unheimlich viele personenbezogene Daten zusammen, werden gespeichert, ausgewertet und vermarktet.
Tracking erschweren

Als ein gegen gewerbliche Datensammler schon recht wirksamen Schritt solltest du sogenannte Cookies sowie Flash-Cookies automatisch löschen lassen. Dabei handelt es sich meist um unserer Person zugeordnete und auf unserem Rechner abgelegte Nummern, die bei jedem Seitenabruf wieder abgefragt und mit deren Hilfe wir selbst von Unternehmen dauerhaft und eindeutig identifiziert werden, die keinen Zugang zu der Zuordnung der verwendeten IP-Adressen zum Kunden haben.

Ein gutes Add-On zum Schutz gegen zu viel Neugier ist Ghostery. Das gibt es fast für alle bekannten Betriebssysteme und Netzbetrachter und sogar für Android- und iOS-Nutzer. Das Netzbetrachter Add-on zeigt nach der Installation oben rechts einen blauen Geist an. Darunter steht eine Ziffer, das ist die Anzahl der momentan verwendeten Webanalyse-Tools einer Weltnetzseite. Wer auf den blauen Geist klickt, sieht im Detail, welche Tools gerade in dieser Sekunde versuchen, dich zu belauschen. Bei jedem Eintrag kann man entscheiden, ob man die Analyse deaktivieren will. Ausgeschaltete Tools erscheinen in rot, die aktiven Tools in blau. Wer die Einstellungen verändert, muss die Seite neu laden. Beim nächsten Besuch hat sich Ghostery unsere Vorlieben gemerkt und

führt die Blockade automatisch durch.

5 Daten-Striptease

In seinen Anfängen wurde das World Wide Web hauptsächlich in der Form genutzt, dass man Inhalte aufrief und eventuell herunterlud. Mit dem Web 2.0 hat sich das geändert. Das Web 2.0 ist ein Mitmach-Netz, dass jedem Nutzer vielfältige Möglichkeiten der Teilnahme bietet. Man konnte sich zwar schon vorher an Chats und Foren beteiligen und per eBrief kommunizieren, aber das Web 2.0 macht es uns so einfach wie nie zuvor, unsere eigenen Inhalte online zu stellen. Ohne technisches Vorwissen kann man eigene Beiträge veröffentlichen, fremde kommentieren, sich virtuell vernetzen oder in Foren präsentieren. Verantwortlich dafür, ist die so genannte Social Software. Obwohl sich die traditionellen Formen der Internetkommunikation immer noch großer Beliebtheit erfreuen, nimmt vor allem bei jüngeren Nutzern die Begeisterung für die Möglichkeit des Web 2.0 zu. Einherr damit geht, ein ungeheurer Exhibitionismus. Für das Web 2.0 scheint nichts peinlich genug zu sein. Schaue dir nur mal die Filmchen auf Youtube an oder lese was in privaten Blogs geschrieben wird (nicht das in Chats ein höheres Niveau herrschen würde). Durch die einfache Handhabung des Web 2.0 kommen gewaltige Datenmassen zusammen, die man zu einem großen Prozentsatz nur noch als Datenmüll bezeichnen kann.

Diejenigen, die sich dort selbst darstellen, sollten sich, bevor sie Videos, Bilder oder Texte einstellen, genau überlegen,ob sie sich nicht selbst Schaden zufügen - vielleicht nicht heute oder morgen, aber auf lange Sicht betrachtet. Je nachdem worum es sich handelt, kann der Schaden auch ziemlich unmittelbar eintreten. Man denke nur an Fotos von Häusern oder Wohnungen. Sie könnten als Material für sog. Outings durch die kriminelle Antifa dienen. Mehr Vorsicht ist in jedem Fall angebracht.

Fünf Fragen, die man sich stellen sollte, bevor man sich im Netz präsentiert:

- Kann man mich identifizieren und finden?
- Können übelwollende Zeitgenossen mir oder anderen Menschen (Verwandten, Freunden) durch die Informationen oder Bilder, die ich hochlade, Schaden zufügen?
- Möchte ich das alles auch in fünf oder zehn Jahren noch irgendwo lesen oder sehen?
- Was möchte ich mit dem was ich einstelle erreichen und ist es ein sinnvolles Projekt?
- Möchte ich, dass meine Eltern, Freunde und mein Arbeitgeber das was ich einstelle, lesen und anschauen können?

Eines sollte jedem Nutzer sozialer Netzwerke klar sein: Sie finanzieren sich durch Mitgliedsbeiträge und verschiedene Formen von Werbung und Sponsorings.

Die Nutzer wollen meistens nicht oder nur wenig zahlen, also ist die Zielgruppen gerichtete Werbung die Haupteinnahmequelle der Betreiber. Dafür sind interessante Informationen über die Nutzer Voraussetzung.

5.1 Grundsätzliche Regeln

(Klar-)Namen

Bei den Communitys, die hauptsächlich für Erwachsene konzipiert worden sind, hat es sich inzwischen etabliert, den vollständigen und echten Namen („Klarnamen“) anzugeben. Facebook startete als Netzwerk für Studenten der Eliteuniversität Harvard. Dort gab man natürlich gerne seinen richtigen Namen an und sah keine Erfordernis in der Verschleierung des eigenen Namens durch ein Pseudonym oder Nicknamen.

Bei den meisten sozialen Netzwerken wird die Nennung des Klarnamens verlangt. Allerdings drücken manche Betreiber eher als andere ein Auge zu, wenn sich jemand offensichtlich mit einem Pseudonym oder einem abgekürzten Namen anmeldet. Google+ hat kurz nach Eröffnung des Angebots zahlreiche Konten unter Verweis auf die eigenen Geschäftsbedingungen gelöscht. Mittlerweile wird dies wohl nicht mehr ganz so streng gehandhabt.
Freunde

Die Anzahl der „Freunde“ in sozialen Netzwerken wird gerade von jüngeren Benutzern oftmals gleichgesetzt mit der Highscore-Liste eines Computerspiels: Je mehr Freunde jemand hat, desto beliebter und bekannter ist er in der Gemeinschaft. Verbergen sich hinter den sogenannten Freunden jedoch nahezu unbekannte Personen, so kann das die zuvor sorgfältig angelegten Sicherheitseinstellungen aushebeln.

Gerade junge Nutzer sollten anfangs nur Freundesanfragen akzeptieren (und stellen), wenn sie sicher sind, dass sie die entsprechende Person auch im echten Leben kennen und ihr persönliche Dinge (wie Handynummer oder Fotoalbum) anvertrauen würden. Möchte man auch den Kontakt zu Personen halten, denen man nicht Zugang zu allen Informationen oder Mitteilungen erlauben möchte, so müssen die Freunde zunächst bestimmten „Listen“ (schülerVZ und Facebook) oder „Kreisen“ (Google) zugeordnet werden. Allen Personen in einer Liste oder in einem Kreis können dann bestimmte Zugangsberechtigungen erteilt werden.
Bilder

Egal, ob schülerVZ, Google+ oder Facebook: Das eigene Profilbild kann bei einem aktiven Konto von allen Mitgliedern der Community eingesehen werden. Wer also in der Community nicht von jedem Mitglied erkannt werden will, sollte sich hier von der kreativen Seite zeigen.

Will man generell in der Community nicht von Fremden erkannt werden, sollte man zudem die Sicherheitseinstellungen so wählen, dass man von anderen Nutzern nicht auf Fotos markiert und verlinkt werden kann. Es bedarf dabei schon einigen Aufwands, um sein Gesicht vor der Community zu verbergen. Insbesondere Facebook macht es durch die automatische Gesichtserkennung seinen Nutzern schwer, nicht auf den Bildern anderer Benutzer erkannt und automatisch verlinkt zu werden, daher gilt hier besondere Vorsicht beim Umgang mit Bildern und den darin enthaltenen „biometrischen Daten“.

Beim Hochladen von Bildern in ein frei zugängliches Fotoalbum ist zudem auf das Urheberrecht und das Recht am eigenen Bild zu achten. Um hier rechtlich abgesichert zu sein sollte man vor dem Upload von Bildern folgende zwei Fragen bejahen können:

1. Sind die abgebildeten Personen damit einverstanden, dass ich das Bild veröffentliche?
2. Ist es wirklich mein Bild, oder habe ich eine ausdrückliche Erlaubnis des Fotografen, das Bild zu veröffentlichen?

Apps

In schülerVZ und Facebook lassen sich zusätzliche Funktionen in Form von Apps nutzen. Diese Anwendungen (z.B. Spiele, Quiz-Module, Chats oder FreundeFinder) sind Angebote von externen Dienstleistern, die zum Teil auch auf die in der Community hinterlegten Nutzerdaten zurückgreifen.

Darüber hinaus benötigen viele dieser Anwendungen weitere personenbezogene Daten des Nutzers.

Auch wenn man eine App nur inerhalb der Community verwendet, so handelt es sich dabei doch um eine eigene, für sich gestellte Anwendung. Die innerhalb der App getätigten Einstellungen berücksichtigen nicht mehr die Einstellungen zur Privatspähere in der Community selbst. Bei der Verwendung solcher Apps muss man also erneut die Preisgabe persönlicher Daten bedenken.

5.2 Schützt eure Daten und Strukturen!

Hält man sich als politischer Aktivist in sozialen Netzwerken wie „facebook“, „youtube“, „twitter“ und „wer-kennt-wen“ auf, wird man bei der Suche nach Gleichgesinnten schnell fündig. Wie einige von politischen Personen jedoch mit sensiblen Daten wie Fotos, Aussagen, Klarnamen und Anschriften umgehen, lässt so manchen Aktivisten nur Kopfschütteln und unsere Gegner Freudensprünge machen. Eine eigene Recherche in virtuellen Netzen...

Es bedarf keiner eingehenden Recherche um bei manchen Personen, die sich politisch engagieren, ein komplettes Nutzerprofil über diesen zu erstellen: Der Eine veröffentlicht jedes Wochenende seine privaten Partyfotos, ein Zweiter teilt der gesamten facebook-Gemeinde, immerhin fast 13 Millionen in der BRD, mit, dass er gerade auf ein politisches Konzert in Frankfurt fährt, ein Dritter zeigt mal eben jedem unter welchem Realbild, Klarnamen, Anschrift und E-Post-Adresse er jederzeit erreichbar ist. Natürlich haben wir kein Recht andere an der Ausübung seiner politischen Arbeit zu kritisieren, aber wenn die persönlichen, wie der Name schon sagt, die persönlichen Daten auch persönlich bleiben.

Wir wollten es herausfinden: Innerhalb von nur wenigen Minuten fand unsere Recherche-Gruppe sechsunddreißig politische Nutzerprofile die derart ungeschützt waren, dass wir uns genötigt sahen den Nutzer anzuschreiben und auf die Schwachstellen hinzuweisen. Circa die Hälfte der Angeschriebenen reagierten verdutzt und versprach ihre Daten besser zu schützen, die eigenen Profile sicherer zu machen. Nach sechs Tagen weiterer Recherche waren diese leider noch immer ungeschützt. Die andere Hälfte der Personen die wir anschrieben, reagierten genau im Gegenteil: Neben wüsten Beschimpfungen, Aussagen wie, dass ≫uns diese Daten nichts angehen≪ bis zu, ≫sie seien politisch aktiv, man sollte auch mal Gesicht zeigen können≪, war fast jede primitive Ausrede dabei. Die Daten jedoch zu schützen - vor dem Zugriff Fremder, kam den Personen jedoch nicht in den Sinn. Ausschließlich zwei Personen reagierten innerhalb einer Woche und sperrten ihre persönlichen Daten erfolgreich.

Zum Schmunzeln, sogar zum laut Auflachen brachten und ganze elf Personenprofile: Bei dem unzensierten Posen neben Fahnen - unnötig zu erklären um welche es sich handelte - natürlich klischeehaft mit Waffe in der Hand, politischen Aussagen die eindeutig unter Strafandrohung stehen, Konzert- und Demofotos - wo mehrere weitere Personen unzensiert gezeigt werden - und „Freundeslisten“, die weder ausgeblendet, was in allen sozialen Netzwerken möglich ist, noch zensiert wurde. Solche Profile sind für politische Aktivisten, und solche die es gerne sein möchten, ein Super-Gau!

Und genau da ist auch Kritik angesagt: Wer mit seinen persönlichen Daten so lasch umgeht, scheint ein Dummkopf zu sein, wer jedoch Personenzusammenhänge, Einzelpersonen, Klarnamen und Gruppen dadurch offen legt, ist ein Zuträger unserer Gegner. Solchen Personen sollte man die Frage stellen ob sie bei einem polizeilichen Verhör auch alles von sich selbst verraten. Sie werden die Frage wohl verneinen, ein Blick auf den Rechner der Person, leichter noch, sein Nutzerprofil bei facebook und schon weiß der übereifrige Systemvertreter wo er sich am letzten Wochenende aufgehalten hat und mit wem er da war. Geschweige denn die „antifaschistische Outing-Gruppe“, die sich bei solchen Daten unterhaltsam freut und bereits die Plakate, Aufkleber und Flugblätter gegen euch - mit euren eigenen veröffentlichten Daten - in Druck gegeben hat. Hinzu kommen

Hausdurchsuchungen, Beschlagnahmungen und Strafverfahren von dem System aufgrund einener Veröffentlichungen, die Repressalien folgen lassen und meistens noch mehr Informationen von uns Preis geben.

Während unser zweistündigen Recherche trafen wir auf über einhundert Nutzer die dem ersten Anblick als politisch RRechtsßu erkennen waren. Neben den Nutzernamen „Rudi Hess“, „Odin 1488“ oder gar „A. Hitler88“ - weitere ersparen wir unseren Lesern um den Lachmuskel zu schonen oder Wutkrämpfe über deren genutzen Nick, deren Schwachsinnigkeit in Verbindung mit hohen, ehrenhaften Persönlichkeiten zu bringen - war deren Einfallslosigkeit grenzenlos. Wir stellten die Suche im Netz frustiert und entäuscht ein, wiesen aber jeden den wir im Netz fanden schriftlich auf das Datenleck seines Profiles hin. Kaum gab es eine Reaktion.

Doch, ist es so schwer die Einstellungen der Netzwerke so zu administrieren, dass die Daten geschützt sind? - Nein, eher noch ist es sinnvoller erst gar nicht über „Privates“ zu plaudern oder zu speichern sondern konzequent von Anfang an seine Internas auch geheim zu halten! Um ein „Gefällt mir“ von Unbekannten in seiner „facebook-Freundesliste“ abzugreifen gibt man auch gerne mal der großen Netzwelt bekannt, dass »er soeben am Bahnhofsvorplatz ein paar Punks mit Tobi und Andy angepöpelt und geboxt hat«. Kurz darauf schreibt Andy, mit Klarnamen darunter - „ja, geile aktion!“ - Zurückverfolgbar in seinem Profil mit voller Anschrift samt Bild. Super, sie wissen wie man mit sensiblen Daten umgeht, meinen wir ironisch. Kopfschütteln bei unseren Recherche-Aktivisten...

Gefestigte, politische Einzelaktivisten und Gruppenführer bekommen bei solchen Nutzerprofilen eine Gänsehaut. Sie fragen sich, wie oft denn noch eine Rechtsschulung durchgeführt werden muss, damit auch der letzte Aktivist mehr Wert auf Datenschutz und Privatsphäre legt. Vielleicht muss auch erst eine Offenlegung der Daten durch einen Gegner erfolgen bis auch der übereifrigste „Kamerad“ erfährt, dass wir uns im Kampf gegen das System befinden und nicht im Umschwung zu einem besseren Leben. Jede Datensammlung der Gegner ist zwar nicht vermeidbar, aber minimierbar auf das Mindeste! Nur durch unsere eigene Dummheit, ja so muss man es schon nennen, können unsere Gegner Zusammenhänge erkennen, Gruppenzugehörigkeiten zusammenreimen und unsere persönlichen Daten speichern und auswerten. Über 60% der Daten über uns werden mittlerweile über solche sozialen Netzwerke gewonnen, wir selbst erleichtern unseren politischen Gegnern ihre Arbeit. Unsere Recherche-Gruppe fand ebenfalls heraus, dass von zehn „Outings“ bundesweit - alleine im letzten Jahr - mindestens acht mit Daten durchgeführt wurden, die wir selbst ihnen, wenn auch unbewusst, per facebook und Co zuspielten. Wie dies geschieht kann sich jeder selbst ausmalen.

Nach dem der „Geoutete“ vielleicht seine Arbeit, Umfeld und Freunde verloren hat, wird nach Schuldigen gesucht und die „Antifa“ als allmächtig angesehen, doch spätestens dann sollte dieser„Kamerad“ sich an die eigene Nase fassen. Oft endet diese Veröffentlichungsaktion der Gegenseite mit einem Austritt aus der Bewegung, weil er scheinbar erst dann begreift, dass wir uns im Kampf mit dem System und seinen Unterstützern befinden und nicht auf einem Abenteuerspielplatz ein bisschen Räuber und Gendarm spielen. Der Vorteil ist, dass nun die Spreu vom Weizen getrennt wird: Keine Öffentlichkeitsmachung von Kameraden ist erfreulich, aber bei Einigen scheint es geradezu unvermeidlich zu sein...

Für politische Personen gibt es bei solchen Nutzerprofilen aber nur eine Konsequenz: Sprecht die Datenoffenleger an, weißt sie auf die sensiblen Daten hin, fordert sie zur Löschung oder öffentlichen Sperrung hin - reagieren sie nicht, ignoriert und isoliert Sie! Kündigt die FFreundschaftenïn den Netzwerken und macht Sie als Datenverbreiter in allen Netzen öffentlich! Wer mit Daten anderer so unachtsam umgeht ist ein Zuträger und wenn auch unbewusster Unterstützer des Systems und hat in unseren Reihen, auch in den virtuellen Netzen, nichts zu suchen! Wer meint, er solle »sein Gesicht zeigen« kann gerne einer unserer Demonstrationen des Widerstandes besuchen statt Maulheld hinter Monitor und Tastatur zu spielen.

Datenschutz ist unvermeidbar - Schützt eure Daten und Strukturen!

5.3 Facebook Sicherheitseinstellungen - Öffentlich vs. Privat

Die Facebook Sicherheitseinstellungen sind immer wieder im Gespräch - Öffentlich vs. Privat. Stetig entwickelt sich Facebook weiter und damit auch die Konfigurationsmöglichkeiten. Folgendes erschreckendes Ergebnis, zeigt das hier noch einiges an Nachholbedarf vorhanden ist:

„(...) After all, more than a quarter of Facebook, users share information with an audience much wider than their social circle. And 13 million users haven t even touched their privacy settings."

Um diese hohe Zahl der Nutzer zu minimieren und für ein höheres Sicherheitsgefüge auf Facebook zu sorgen dient dieser Beitrag, rund um das Thema Facebook und die (richtigen) Sicherheitseinstellungen.

Mit der Einführung des neuen Facebook Graph-Search und den neuen Facebook-Profilen empfiehlt es sich gleich doppelt, die aktuellen Sicherheitseinstellungen zu überprüfen.

5.4 Allgemeine Einstellungen

Auf Facebook gibt es 2 wichtige Seiten bezüglich der Einstellungen. Da wäre zum Einen der Menüpunkt „Kontoeinstellungen" und zum Anderen der Punkt „Privatsphäre-Einstellungen" - beides zu finden, in dem man auf den rechts oben liegenden Pfeil klickt.

Unter dem Punkt Allgemein findet sich eine Option „Lade eine Kopie deiner Facebook-Daten herunter." Dort kann man im Falle einer Kontenlöschung diverse Dinge wie das eigene Profil, Namen der Freunde, Bilder, uvm. absichern. Leider bietet Facebook keine Option diese Daten wieder zu importieren - man muss also alles händisch wieder nachtragen.
Das Facebook Passwort sollte alle 3 Monate gewechselt werden.

5.5 Privatsphäre-Einstellung

Hier ist vorallem folgendes einzustellen:
Mit einem Klick auf Benutzerdefiniert, öffnet sich ein Dialogfenster, in dem man einstellen kann, welche Listen und/oder Personen Deine Statusmeldungen lesen kann. Wie man sehen kann wurde im Beispiel eine Liste „Kameraden" erstellt. Das kann aber jeder nach eigenen Bedürfnissen einstellen. Abschließend klickt man auf „Einstellung speichern".

Darunter befinden sich nun noch viele weitere Optionen:

Da sämtliche Einstellungen dort gut erklärt werden, ist es hier nur nötig darauf hinzuweisen. Es ist empfehlenswert alle aufgelisteten Möglichkeiten einmal anzuklicken und zu schauen, was man dort einstellen kann und wie man es gerne eingestellt haben möchte.

Um nachzuprüfen, wie bestimmte Leute Dein Profil und Deine Statusmeldungen sehen, kannst Du in Deiner Profilseite oben rechts auf „Anzeigen aus der Sicht von..." klicken, Namen eingeben und prüfen.

5.6 Die richtigen Sicherheitseinstellungen für Twitter

Zuerst gehst du auf die Weltnetzseite von Twitter und loggst dich mit deinem Account ein. Nun klickst du auf das Zahnrad in der oberen rechten Ecke. Dadurch öffnet sich ein Menü. In diesem Menü wählst du den Punkt Einstellungen aus.

Hier gibt es nun zwei Einstellungen die für uns interessant sind. Das währe als erste die Einstellung „Standort twittern“. Ähnlich wie bei Facebook, Google+ und den meisten anderen Social Apps auf deinem Smartphone, kannst du auch bei Twitter einstellen, dass dein Standort mit angezeigt wird. Diese Funktion sollte meiner Meinung nach deaktiviert sein. Vorallem wenn du wirklich viel twitterst. Es ist hier genau so möglich ein Bewegungsprofil zu erstellen wie mit allen anderen Apps die deinen Standort preisgeben.

Die zweite Option auf die ich hier eingehen möchte ist „Meine Tweets schützen“. Mit dieser Option kannst du festlegen, dass nur Personen die du zuvor bestätigt hast, auch deine Tweets bekommen. Auch eine nützliche Option, denn nicht jeder will sich Gott und der Welt mitteilen. Wie auch an deinem Computer empfehlen wir Twitter, wie jedes andere „soziale Netzwerk“, ausschließlich über eine sichere Verbindung zu besuchen. Wenn du die Twitter App auf deinem Mobiltelefon installiert hast solltest du dir diesen kurzen SfN Blogartikel über die Smartphone-Sicherheit durchlesen.

6 Tracking verhindern

Was verrät unser Netzbetrachter eigentlich alles über uns? Beim Besuch einer Weltnetzseite wird weitaus mehr als nur die IP-Adresse übertragen. Die moderne Webanalyse erlaubt sogar anhand der hinterlassenen Spuren das Ausforschen all unserer Vorlieben.

Um deine Weltnetzseitenaufrufe auszuforschen und Profile über dich anzulegen wirst du regelrecht verfolgt. Sogenannte Datenkraken wie z.B. Google, speichern nicht nur beinahe jede Eingabe und jeden Klick bei der bewussten Nutzung der Google-Dienste, sondern verfolgen und speichern möglichst jeden mit technischen Tricks ausgeforschten Seitenabruf auch außerhalb der eigenen Dienste.

Schützt du dich nicht gegen solches Tracking, erleichterst du das Anlegen und den potenziellen Missbrauch von sehr umfangreichen Profilen zu deiner Person, Arbeit und/oder Institution.
Große Datenkraken lieben kleine Kekse: Verräterische Cookies

Um dich dauerhaft verfolgen und eindeutig identifizieren zu können, vergeben solche Schnüffler dazu u.a. eine dir zugeordnete Nummer, die im Hintergrund in einem sogenannten Cookie auf deinem Computer gespeichert und bei jedem der weiteren Abrufe wieder an die Schnüffler übertragen wird und diesen damit auch unabhängig von den unter Umständen wechselnden IP-Adressen oder Internetzugängen mitzuteilen, wer was abruft und damit, welches Profil weiter gepflegt werden soll.

So können über Jahre hinweg alle Suchen und Seitenabrufe diesen eindeutigen Nummern zugeordnet werden. Diese Nummern können wiederum - z.B. durch im Laufe der Zeit erfolgte Logins, anhand bestimmter IP-Adressen, den Spuren auf deinem Computer oder bestimmter Suchen oder Verhaltensmuster - mit deiner Person in Verbindung gebracht werden.

Um dich also vor langfristigem Nachstellen zu schützen, solltest du:

- Cookies mindestens bei jedem Beenden deines Browsers löschen lassen und Cookies auch nur den Seiten erlauben, die du gerade aufgerufen hast
- sich auch vor ähnlich funktionierenden Flash-Cookies schützen

- in viele Seiten eigebetetten und bei der Ausführung Daten sammelnde JavaScripts von Trackingdiensten wie Google-Analytics blocken

Du erreichst dies z.B. mit folgenden Einstellungen:
Nach dem ersten Start von Firefox gehst du im Menü auf Extras ¿ Einstellungen ¿ Datenschutz. Dort machst du einen Haken bei Websites mitteilen, dass ich nicht verfolgt werden möchte. Bei dem Punkt Adressleiste, der nichts anderes ist als die Chronik der Besuchten Weltnetzseiten, hast du 3 Einstellungsmöglichkeiten. Wir empfehlen dir Niemals eine Chronik anzulegen.
Nun springst du weiter zu dem Reiter Sicherheit. Hier machst du, falls vorhanden, die Haken aus den Kästchen Passwörter speichern und Master Passwort verwenden raus. Mit OK kannst du das Fenster jetzt schließen.
Willst du nicht auf den Komfort einer Chronik verzichten empfehlen wir dir auf eine Portable Version des Firefox umzusteigen.

6.1 Flash-Cookies und Super-Cookies löschen lassen

Außerdem solltest du unbedingt auch Flash-Cookies und Super-Cookies berücksichtigen!

Das Plugin "BetterPrivacyßchützt dein System vor hartnäckigen Cookies. Die sogenannten Flash-Cookies nisten sich unbemerkt auf deinem Computer ein und können deine Aktivitäten am Computer erfassen. Mit dieser Erweiterung hast du die Möglichkeit, solche Eindringlinge automatisch entfernen zu lassen.

Hier gezeigte Programmversion: 1.68
Als erstes öffnest du den Firefox Netzbetrachter, gehst auf Extras und klickst dann auf Add-ons.

Es hat sich nun der Add-ons-Manager geöffnet und du gibst in das Suchfeld BetterPrivacy ein und bestätigst mit Enter.

An der ersten Stelle ist auch schon das gesuchte Add-on. Nach einem Klick auf Installieren läd Firefox das kleine Helferlein herunter und installiert es.

Nach der Installation muss der Firefox Netzbetrachter neu gestartet werden damit das Add-on aktiv wird.

Möchtest du die Einstellungen der Add-On sehen gehst du auf Extras ¿ Add-ons und klickst dort auf Erweiterungen.

Hier werden dir alle Add-Ons die du installiert hast angezeigt und du kannst dir die Einstellungen ansehen, sie deaktivieren oder deinstallieren.

In den Einstellungen dieser Add-On musst du aber nichts verändern. Die hartnäckigen Cookies werden nun mit jedem Beenden des Netzbetrachters automatisch gelöscht.

6.2 Seitenübergreifende Dienste

Problematisch sind weiterhin seitenübergreifende Dienste wie Google-Ads, Google-Analytics, Twitter- oder Facebook-Buttons (sogenannte Gefällt mir Buttons), da diese nicht vom Anbieter der Weltnetzseite sondern immer direkt von wenigen Unternehmen geladen werden, die damit über den Besuch der Seiten informiert werden.

Tracker sind leider in den seltensten Fällen so offensichtlich wie die „Gefällt mir“ Buttons. Am weitesten verbreitet ist „Google Analytics“, eine von Google bereitgestellte Software, welche zur

Erstellung von Statistiken über die Nutzung einer Webseite dient. Bindet ein Betreiber diesen Dienst ein, werden die Daten zentral von Google erfasst und ausgewertet. Dadurch kann Google in Verbindung mit vielen anderen Quellen, Profile der Benutzer erstellen.

„Ghostery" ist ein Plug-In welches für die meisten Netzbetrachter (Internet Explorer, Firefox, Safari, Opera, Chrome) verfügbar ist. Es enthält eine Liste der gängigsten Tracker und wird ständig aktualisiert. Leider erfordert es ein kleines bisschen Konfiguration, dafür schützt es aber sehr zuverlässig vor den meisten Trackern. Da wir den Netzbetrachter Firefox verwenden und empfehlen und dieser eine große Akzeptanz genießt, beschreiben wir hier die Installation für genau diesen Netzbetrachter.

Hier gezeigte Programmversion: 2.8.3
Du öffnest den Firefox Netzbetrachter, gehst auf Extras und klickst dann auf Add-ons. Im nun erscheinenden Add-On Manager suchst du nach ghostery.

Ghostery sollte in der Liste ganz oben auftauchen. Klicke hier auf Installieren.

Nachdem der Download abgeschlossen wurde, klicke auf Jetzt neu starten um die Software zu installieren.
Sicherheit2
Nach dem Neustart von Firefox bietet dir Ghostery einen Assistenten an. Diesen verwenden wir nicht, klicke deshalb auf Assistenten überspringen. Du findest nun rechts oben neben der Suchleiste ein neues Icon welches einen kleinen Geist darstellt. Klicke auf dieses Icon und wähle Optionen.
Es öffnet sich die Konfigurationsseite von Ghostery. Als erstes aktivierst du das Blockieren aller bekannten Tracker. Relativ weit unten auf der Seite gibt es eine Auflistung, die wie folgt aussieht.

Klicke hier auf Select all. Es sollte nun bei „XXX total Zählpixel" und „(XXX blocked)" der gleiche Wert stehen. Anschließend wählst du auf den Reiter Cookies und klickst dort ebenfalls Select all.

Bewege dich nun zurück nach ganz oben auf der Seite. Dort befindet sich neben General, der Reiter Advanced. Klicke auf diesen für weitere Optionen.

Mit dem ersten Eintrag unter Allgemeine Optionen bestimmst du, ob Ghostery beim Besuch jeder Webseite ein kleines Fenster einblenden soll, welches die erkannten Tracker auflistet. Dieses Fenster sieht wie folgt aus (durchgestrichene Tracker wurden blockiert).

Die Einstellung dazu heißt Warnmeldung einblenden. Wenn du dieses Information nicht möchtest, kannst du den Haken gefahrlos entfernen.

Eine sehr wichtige Option, die etwas weiter unten auf dieser Seite zu finden ist, nennt sich Block new elements by default und findet sich unter der Rubrik Auto Update.

Die Liste der von Ghostery erkannten Tracker wird ständig erweitert und automatische aktualisiert. Damit neue Einträge auch gleich blockiert werden, solltest du den Haken hier auf jeden Fall setzen!

6.3 Fingerabdruck des Netzbetrachters

Problematisch bliebe dann noch der leider relativ individuelle Fingerabdruck des Netzbetrachters. Diesen hinterlässt jeder Netzbetrachter beim Aufrufen einer Weltnetzseite, indem er Informationen über Betriebssystem, Netzbetrachtertyp, Zeitzone und Bildschirmeinstellungen sowie über installierte Plugins, Software zur Medienwiedergabe und Schrifttypen preisgibt. Diese Daten sind mehr oder weniger einzigartig. Aus allen gewonnenen Daten lässt sich dann der Fingerabdruck erstellen.

Ein Fingerabdruck lässt sich nutzen, um deinen Netzbetrachter beim erneuten Besuch einer Weltnetzseite zu identifizieren und diese Information beispielsweise für Werbung zu nutzen. Solange sich daran nichts ändert, bleibt der Fingerabdruck gleich. Es genügt aber eine neue Version eines Add-Ons zu installieren und der Fingerabdruck ändert sich.

Für einen Fingerabdruck werden u.a. diese Daten ausgewertet. (extrem vereinfacht)

- Systemzeit: Tue Feb 28 2017 16:35:06 GMT+0000 (UTC)
- Plattform: Win32
- Aufloesung: 1039 x 900
- Farbtiefe: 24 bit
- Cookies aktiviert: ja
- JavaScript aktiviert: Ja
- Java aktiviert: nein
- Installierte Plugins:

Was dein Netzbetrachter noch über dich verrät kannst du dir auf der Seite: **www.ip.s-f-n.org** ansehen. Dort werden die Daten nur angezeigt und natürlich nicht gespeichert oder verwendet.

Die Bürgerrechtsorganisation Electronic Frontier Foundation hat einen Dienst veröffentlicht, mit dem Weltnetz-Nutzer herausfinden können, wie einzigartig ihr Netzbetrachter ist. Interessant ist das in erster Linie für Personen, die um Datenschutz und Identifizierbarkeit im Netz besorgt sind. Außer über Cookies, Session-ID oder IP-Adresse ermöglicht der Fingerabdruck des Netzbetrachters unter Umständen recht zuverlässig, seinen Besitzer zu erkennen.

Die EFF-Anwendung Panopticlick sammelt anonymisierte Daten, um den Nutzern bei der Einschätzung zu helfen, wie leicht sie in der Menge der Surfer erkannt werden können. Der Dienst wertet die HTTP-Anfrage-Header aus (Netzbetrachterkennung und akzeptierte MIME-Typen) und versucht, mittels JavaScript Informationen über installierte Add-Ons, Plug-Ins, Schriftarten, die Bildschirmgröße und die Zeitzone zu ermitteln; zuletzt fließen auch Daten über Standard- und „Supercookies“ (Web Storage, Flash-Cookies, IE-userData) in das Ranking ein. Derzeit hat die EFF etwa 200.000 Datensätze zum Vergleich gesammelt. Interessanter Nebeneffekt des Projekts: Die Daten erlauben Aufschluss darüber, wie verbreitet beispielsweise Bildschirmauflösungen und Supercookies sind.

Nicht selten identifiziert der Test einen Netzbetrachter sogar eindeutig - vor allem, wenn der Anwender mit einem weniger verbreiteten Netzbetrachter auf einem Nicht-Windows-System unterwegs ist. Doch man muss nicht unbedingt mit Internet Explorer 7 auf Windows XP und mittelgroßem Monitor surfen, um keine eindeutigen Fingerabdrücke zu hinterlassen.

Betriebssystem und Netzbetrachter-Version erhält der Test aus der Netzbetrachter-Kennung, die sich bei vielen Netzbetrachtern gezielt ändern lässt - etwa bei Firefox mit dem User Agent Switcher. Die detailliertesten Informationen ergeben sich aus den installierten Add-Ons und Plug-Ins und Fonts (auf dem Computer installierte Schriftarten), die der Test via JavaScript ermittelt. Das Abschalten von JavaScript reduziert die Menge der ermittelbaren Informationen somit deutlich. Das lässt sich mit NoScript auch seitenspezifisch reglementieren. Bereits mit diesen einfachen Maßnahmen tauchte ein vorher eindeutig zu identifizierender Netzbetrachter in einer Menge von etwa 30.000 gleichartigen Systemen unter - die sich ohne Proxy allerdings immer noch an Hand der IP-Adresse unterscheiden ließen.

Canvas Fingerabdruck

Seit html5 gibt es die Tracking-Methode des Canvas Fingerabdruckes. Der Trick ist der: Man lässt den Netzbetrachter eine Grafik zeichnen. Canvas genannt. Erzeugt mit Programmcode, der im Netzbetrachter läuft - also direkt auf dem eigenen Computer. Da, wie oben schon beschrieben wurde, jedoch jeder Computer aber ein bisschen anders ausgestattet ist, sehen die Bilder nicht immer gleich aus. Vor allem bei erzeugten Schriftzügen gibt es kleine Unterschiede im Ergebnis. Diese Unterschiede sind kaum zu sehen, lassen sich aber dennoch messen - und werden in einen eindeutigen Code umgerechnet. Dieser Fingerabdruck bleibt immer gleich.
Und schon ist man als Benutzer erkennbar und unterscheidbar

Natürlich werden keine so großen Grafiken auf dem Bildschirm gezeichnet, nur um den Fingerabdruck auszurechnen. Die Grafiken sind deutlich kleiner - und sogar unsichtbar. Man merkt also gar nicht, wenn diese Art von Fingerabdruck genommen wird. Diese neue Methode ist äußerst effektiv - und sie wird natürlich auch eingesetzt.

Es ist nicht einfach, als Benutzer Canvas Fingerprinting zu verhindern - aber es ist möglich. Weiterhelfen kann eine kostenlose Netzbetrachter-Erweiterung wie NoScript. Wenn man die geladen hat, dann kann man selbst bestimmen, welche Weltnetzseiten Scripte ausführen dürfen und welche nicht. Werbenetzwerken kann man es zum Beispiel verbieten. Das ist allerdings nicht immer ganz einfach zu entscheiden - und auch ein bisschen mühselig. Die Erweiterung CanvasBlocker blockt bereits die neuen Tracking-Tricks. Auch der Werbeblocker AdBlock Plus kann weiter helfen, allerdings nur mit der Liste EasyPrivacy und wenn er korrekt eingestellt ist. Für wirklich zuverlässige Nichtverfolgbarkeit hilft aber tatsächlich nur das

Tor Netzwerk mit dessen Hilfe der Fingerabdruck verfälscht wird.

7 Das Tor-Netzwerk

Frei verfügbar zum herunterladen hier: **www.torproject.org**
Viele gute Gründe sprechen dafür, seine Identität im Weltnetz zu verschleiern. Dabei hilft das Tor-Netzwerk im Verbund mit dem passenden Content-Filter.

Tor ist ein kostenloses Netzwerk zur Anonymisierung von Verbindungsdaten. Es nutzt ein weltweit verteiltes Netz von 2400 Nodes. Aus diesem Pool werden jeweils drei Nodes für eine Route ausgewählt. Diese Route wechselt alle 10 Minuten. Die zwiebelartige Verschlüsselung sichert die Anonymität der Kommunikation. Selbst wenn zwei Nodes einer Route kompromittiert wurden, ist eine Beobachtung durch Dritte nicht möglich.

Da die Route ständig wechselt, müsste ein großer Teil des Netztes kompromittiert worden sein, um einen Zusammenhang von Benutzer und angefragter Weltnetzseite herstellen zu können. Die weltweite Verteilung der Nodes und der hohe Anteil privater Computer mit langsamer Internetanbindung kann zu deutlich langsameren Downloads führen.

Tor ist neben Surfen auch für IRC, Instant-Messaging, den Abruf von Mailboxen oder Anderes nutzbar. Dabei versteckt Tor nur die IP-Adresse.
Für die sichere Übertragung der Daten ist SSL- oder TLS-Verschlüsselung zu nutzen.

Sonst besteht die Möglichkeit, dass sogenannte „Bad-Exit-Nodes“ die Daten belauschen und an Userkennungen und Passwörter gelangen.

Man kann davon ausgehen, dass die Geheimdienste verschiedener Länder ebenfalls im Tor-Netz aktiv sind und sollte die Hinweise zur Sicherheit beachten:

- sensible Daten nur über SSL-verschlüsselte Verbindungen übertragen
- SSL-Warnungen nicht einfach wegklicken
- Javascript deaktivieren

Dann ist Tor für anonyme Kommunikation geeignet.

7.1 Funktionsweise von Tor - Was steckt dahinter?

Tor steht als Abkürzung für „The Onion Routing“ - ein Projekt, das von der US-Marine initiiert und umgesetzt wurde, um die Kommunikation innerhalb der Regierung zu schützen.

Der Tor-Client, verteilt die Transaktionen des Nutzers über mehrere verschiedene Stellen im Weltnetz und sorgt dafür, dass die Identität des Benutzers an keiner Stelle mit der Kommunikation in Berührung kommt. Die Datenpakete verwenden dazu einen zufällig ausgewählten Weg über Server im Tor-Netzwerk. Dabei wählt Tor die Route eines Datenpakets immer so, dass es über drei Server verschickt wird. Diese Route wird von Tor alle 10 Minuten geändert. Eine solche Route wird auch „Kanal“ genannt.

Als erstes verbindet sich der Tor-Client, mit dem Tor-Netzwerk und lädt sich eine Liste aller vorhandenen und nutzbaren Tor-Server herunter. Diese Liste ist mit einer digitalen Signatur versehen und wird von Verzeichnisservern, zur Verfügung gestellt. Die öffentlichen Schlüssel der Verzeichnisserver werden mit dem Tor-Quellcode geliefert und stellen sicher, dass der Tor-Client nur authentische und keine modifizierten Verzeichnisse erhält.

Durch die erhaltene Liste weiß der Tor-Client nun welche vorhandenen und nutzbaren Tor-Server zur Verfügung stehen.

Möchtest du jetzt z.B. die Weltnetzseite von uns erreichen wählt der Tor-Client eine Route über genau drei Tor-Server, um ein möglichst optimales Verhältnis zwischen großer Anonymität und akzeptabler Performance zu erreichen. Dabei verhandelt er mit dem ersten Tor-Server (engl. entry node) eine verschlüsselte Verbindung aus. Ist diese aufgebaut, dann wird sie um einen weiteren sicheren Server ergänzt.

Ein Tor-Server kennt immer nur seinen direkten Vorgänger und seinen direkten Nachfolger. Das heißt kein Tor-Server kennt jemals den gesamten Pfad.
Der Client handelt für jeden Schritt entlang des Pfads einen eigenen Satz von Verschlüsselungsschlüsseln aus und stellt damit sicher, dass kein Server die Verbindungen nachvollziehen kann, während sie bei ihm vorbeikommen. Die Anonymität ist nur dann gewährleistet, wenn mindestens einer der drei Server vertrauenswürdig ist und die Anfangs- und Endpunkte der Kommunikation nicht überwacht werden. Der letzte Server in der Route wird als Exit-Knoten (engl. exit node) bezeichnet. Er erhält eine besondere Rolle in dem Konstrukt. Tor bietet sicherlich kein Patentrezept für sicheres Surfen, legt jedoch die Messlatte für Schnüffler und Angreifer sehr hoch. Da das System dezentral arbeitet, ist es wesentlich widerstandsfähiger gegen An- und Übergriffe als andere Anonymisierungsdienste. Darüber hinaus bietet das Design des Onion-Routing im Moment das sicherste Mittel, das Netz anonym zu nutzen: Das Arbeitsprinzip zu kompromittieren, setzt einen erheblichen Aufwand voraus, der auch dann nicht zwangsläufig von Erfolg gekrönt ist.

Galt Tor noch vor wenigen Jahren aufgrund seiner niedrigen Transferraten als weitgehend unbenutzbar, hat sich das Bild zwischenzeitlich deutlich gewandelt. Im Test lag der durchschnittliche Datendurchsatz bei etwa 60 KByte/s, was zum Surfen vollkommen ausreicht, bei größeren Downloads aber die Geduld des Nutzers strapaziert. Allerdings ist das Tor-Netzwerk für solche

Anwendungsfälle auch gar nicht vorgesehen.

7.2 Gefahren des Tor-Netzwerks - Was muss beachtet werden?

Unverschlüsselte Endverbindungen (kein SSL/TLS)

Die Kommunikation innerhalb des Tor-Netzwerk läuft zwar stets verschlüsselt ab, jedoch ist die Verbindung vom Exit-Knoten zur angeforderten Weltnetzseite logischerweise unverschlüsselt. Das bedeutet, dass man bei der Verwendung von Tor immer auf eine Ende-zu-Ende Verschlüsselung setzen sollte. Das heißt nichts anderes als darauf zu achten, dass beim Eingeben von Passwörter oder beim Übertragen von persönlichen Daten (z.B. in Formularen) immer ein „https“ statt einem „http“ in der Adresszeile steht und das dazugehörige Zertifikat authentisch ist. Denn nur dann werden die Daten über SSL/TLS verschlüsselt übertragen. Wer diesen Punkt nicht beachtet, verliert nicht nur seine Anonymität, sondern sogar seine Daten!
Bei der Übertragung von Benutzernamen und Kennwörtern, wie es z.B. bei der Anmeldung oder Registrierung an einem Service geschieht, gilt also folgendes:

Falsch

http://www.altermedia-deutschland.info
http://www.amazon.de
http://www.ebay.de
http://www.fsn.tv.de

Richtig

https://www.altermedia-deutschland.info
https://www.amazon.de
https://www.ebay.de
https://www.fsn.tv.de

Versehentliche Identifikation über Plugins und Add-Ons

Manchmal trügt der Schein und die eigentlich vorhandene Anonymität des Tor-Netzwerks wird über externe Hebel außer Kraft gesetzt.
Denn obwohl der Benutzer das Tor-Netzwerk verwendet besteht die Möglichkeit, dass er sich über Netzbetrachter Add-Ons, wie zum Beispiel Java, Flash, ActiveX, RealPlayer, Quicktime, Adobe PDF und andere Plugins und Add-Ons (Google Toolbar) identifiziert. Denn diese Erweiterungen können so manipuliert werden, dass sie die wahre IP-Adresse anzeigen. Du solltest auch im Tor-Browser nur die von uns beschriebenen Add-Ons installieren, auf jedenfall aber NoScript Aktivieren. Dazu aber später mehr.

7.3 Das richtige Paket - Installation und Inbetriebnahme

Tor muss nicht mehr mühsam Schritt für Schritt installiert werden. Du musst nur die Datei runterladen, sie extrahieren (entpacken) und in dem nun neuen Ordner auf Start Tor Browser drücken.

Auf der Weltnetzseite vom Tor-Projekt gibt es zahlreiche Pakete von Tor. Von der Vielfalt sollte man sich aber nicht verunsichern lassen und sich an folgende Regeln halten:

- Das richtige Betriebssystem wählen

- Nur die stabilen Versionen runterladen
- Das Tor-Bundle runterladen (auch „Tor-Browser-Bundle“ genannt)

Am besten lädst du dir das Komplettpaket herunter, und extrahierst es auf einen USB Stick. So kannst du Tor an jedem Computer benutzen ohne etwas neu installieren zu müssen.

Das Tor-Paket enthält:

- Tor-Software (portable)
- Firefox (portalble)
- Polipo
- Vidalia

Der Start

Polipo und Vidalia sind Zusatzprogramme die den Datenverkehr noch sicherer und anonymer machen sollen. Gestartet wird das Ganze dann direkt vom USB-Stick.

Dazu im Startorder „Tor-Browser“ auf „Start Tor Browser“ klicken. Es öffnet sich ein Fenster und Tor fragt dich als erstes ob du eine Verbindung Aufbauen möchtest oder ob du noch einstellungen vornehmen möchtest. Die Einstellungen musst du im Regelfall nicht ändern also klickst du gleich auf Connect

Jetzt beginnt Tor sich mit dem Netzwerk zu Verbinden.

Sobald die Verbindung hergestellt ist, öffnet sich nach wenigen Sekunden die portable Version des Firefox Netzbetrachter und es erscheint im Startfenster eine grüne Zwiebel und daneben steht „Congrulations! This browser is configured to use Tor.“

Siehst du diese Weltnetzseite in dem Netzbetrachter ist er erfolgreich mit dem Tor-Netzwerk verbunden und du kannst nun anonym durchs Weltnetz „surfen“. Auf www.ip.s-f-n.org kannst du dir jetzt ansehen mit welcher IP Adresse du dich im Weltnetz bewegst und aus welchem Land dieser Erde diese kommt. Wichtig ist, dass du NUR diesen Netzbetrachter benutzt. Nur der Tor-Browser ist richtig eingestellt um anonym zu surfen. Benutze nicht deinen Standardbrowser, da dort bestimmte Einstellungen fehlen!

In den Einstellungen im Startmenü kann man Tor natürlich auch auf deutsch umstellen. Sicherheitslücke durch veraltete Tor-Browser Versionen:

Scheinbar seltsam unbeachtet unter Aktivisten, ist kürzlich ein schwerwiegender Angriff der US-amerikanischen Spitzelbehörde NSA (National Security Agency) auf den Anonymisierungsservice Tor bekannt geworden. Unter dem altbekannten Deckmantel des Kampfes gegen Terror und Kriminalität sind vermutlich einige tausend Benutzerdaten von Tor-Benutzern über die Ausnutzung einer Schwachstelle des Anonymisierungsnetzwerkes ermittelt worden. Nach dem jetzigen Kenntnissstand handelt es sich bei den ermittelten Daten um den Hostnamen (der Gerätename) und die IP-Adresse, welche in Kombination eine relativ sichere Identifizierung des Benutzers ermöglichen.

Betroffen sind dabei Nutzer, für welche ALLE der drei folgenden Kriterien zutreffen:

- Aufrufen einer Weltnetzseite, die von „Freedom Hosting“ gehosted wurde (Tor-Onionland)
- JavaScript war aktiviert

- Verwenden einer Version des Tor-Browser-Bundle (TBB) niedriger als Version 17.0.7.

Man kann vermutlich auch sagen, dass nur Windowsnutzer betroffen sind, wobei sich jedoch niemand aufgrund eines anderen Betriebssystems sicher fühlen sollte.

Halte also das Tor-Browser-Bundle immer aktuell um gefährliche Sicherheitslücken zu vermeiden!

Spätestens wenn du nach dem Starten des Tor-Browsers dieses Fenster siehst solltest du deinen alten „Tor-Browser“ Ordner löschen und dir das ganze Paket neu herunterladen.
Tor beschleunigen:

Tor kann die Surfgeschwindigkeit sehr beeinträchtigen, da die Verbindungen über die ganze Welt geleitet werden können. Folgendes sollte möglicherweise etwas Abhilfe schaffen:

Links oben im Tor-Browser klikst du auf die Zwiebel und in dem sich öffnendem Fenster auf New Identity. Damit sucht Tor nach neuen Verbindungen, die möglicherweise schneller sein könnten. Wenn es nicht klappt, einfach nochmal probieren.

7.4 Tor-Browser richtig einstellen

Der Tor-Browser ist für anonymes Surfen konfiguriert. Tracking-Spuren und Werbung sehen die Entwickler nicht als Problem, da der Datenverkehr anonymisiert ist. Ich empfehle einige Anpassungen, um überflüssige Spuren im Netz zu minimieren.

JavaScript deaktivieren

TorProject.org empfiehlt in den offiziellen FAQ JavaScript nicht zu deaktivieren.

However, we recommend that even users who know how to use NoScript leave JavaScript enabled if possible, because a website or exit node can easily distinguish users who disable JavaScript from users who use Tor-Browser bundle with its default settings (thus users who disable JavaScript are less anonymous).

Ein Test mit Panopticlick lässt aber das Gegenteil als sinnvoll vermuten.

Mit aktiviertem JavaScript:

Within our dataset of several million visitors, only one in 33,726 browsers have the same fingerprint as yours.

Die Tabelle der ausgewerteten Features zeigt, dass (bei mir) die per JavaScript ausgelesene Bildschirmgröße den höchsten Informationswert hat. Genau dieses Merkmal wird von der Google Suche ausgewertet oder von Trackingdiensten wie Multicounter als individuelles Merkmal registriert

JavaScript deaktiviert:

Within our dataset of several million visitors, only one in 2,448 browsers have the same fingerprint as yours.
Die Tabelle der ausgewerteten Features:

Auch wenn Panopticlick einer wissenschaftlichen Untersuchung nicht standhält und auch manipulierbar ist, sind die Ergebnisse mit Unterschieden von mehr als einer Zehnerpotenz ein deutlicher

Hinweis. JavaScript ermöglicht das Auslesen vieler Informationen, die zu einem individuellen Fingerprint verrechnet werden können. Auch ein bösartiger Exit-Node könnte diese Informationen erlangen, wie TorProject.org in den FAQ erwähnt.

JavaScript sollte allgemein verboten werden und nur für vetrauenswürdige Weltnetzseiten freigegeben werden. Weitere Infos: Script - Infoseite

Der Tor-Browser hat das Add-On NoScript integriert, es wartet nur darauf von dir eingeschaltet zu werden.

Werbung und Trackingscripte blockieren

Das Tor-Browser-Bundle enthält keinen Werbeblocker. TorProject.org argumentiert, dass mit einem Werbeblocker das Weltnetz gefiltert wird und jede Filterung lehnen die Entwickler grundsätzlich ab. Außerdem möchte TorProject.org nicht in den Ruf kommen, Geschäftsmodelle im Weltnetz zu stören. Als drittes könnten möglicherweise unterschiedliche Filterlisten als Merkmal für den Browserfingerprint genutzt werden. Es gibt allerdings bisher keine wissenschaftlichen Untersuchungen, die diese Vermutung belegen oder entkräften.

Das Blockieren von Werbung reduziert nicht nur die Belästigung. Da das Tor-Netz langsam ist, wird auch der Seitenaufbau beschleunigt, wenn überflüssige Daten nicht geladen werden.

Empfehlenswert ist die Installation von AdBlock Plus. Nach der Installation kann man die Liste Easylist Germany + Easyprivacy abonieren. Cookies und EverCookies

Der Tor-Browser akzeptiert standardmäßig Cookies von der aufgerufenen Weltnetzseite und lässt EverCookie Markierungen zu. Ein Ändern der Einstellungen zur Annahme von Cookies empfehle ich nicht. Viele Webdienste nutzen EverCookie Techniken zum Tracking, wenn Cookies gesperrt wurden.

Man sollte dem Anonymitätskonzept des Tor-Browser folgen und bei Bedarf gelegentlich alle Identifikationsmerkmale löschen. Alle Cookies und alle bekannten EverCookie Markierungen werden beim Beenden des Netzbetrachters gelöscht oder wenn man den Menüpunkt „Neue Identität“ der Zwiebel in der Toolbar wählt.

5TorEinstellen4
Insbesondere vor und nach dem Login bei einem Webdienst sollte man alle Markierungen entfernen, um eine Verknüpfung des Surfverhaltens mit Accountdaten zu verhindern. Tor-Browser-Bundle mit weiteren Anwendungen nutzen

Im Tor-Browser-Bundle startet Vidalia den Tor-Daemon mit einem zufällig gewählten SOCKS Port und teilt diesen Port nur dem Tor-Browser mit. Alle anderen Programme können den Tor-Daemon nicht erreichen. Wenn man diesen Tor-Daemon nicht nur mit dem Tor-Browser sondern auch mit einem eBrief-Client oder Instant-Messaging-Client nutzen möchte, muss man dieses Verhalten ändern und einen festen SOCKS Port vorgeben.

In den Einstellungen von Vidalia ist die Option „Konfiguriere den Kontroll-Port automatisch“ auf dem Reiter „Fortgeschritten“ zu deaktivieren. Dann lauscht der Tor-Daemon am Port 9150 für andere Anwendungen und nutzt den Kontroll-Port 9151 für die Kommunikation mit Vidalia.

5TorEinstellen5

7.5 Spezielle Tor-Browser

Wenn du Tor benutzen willst, den Firefox aber nicht magst, kann du dir auch spezielle Tor-Browser herunterladen.

Die bekanntesten sind die Opera Tor-Browser und XeroBank. Diese Netzbetrachter haben Tor schon mit installiert und sind auch schon perfekt eingestellt. Zudem verfügen sie über zahlreiche Tools die später im Hintergrund laufen und uns noch mehr Sicherheit verschaffen. Wir empfehlen definitiv das Nutzen des original Mozilla Firefox.

7.6 Tor-Bad-Exits

Ein sogenannter „Bad-Exit-Node“ im Tor-Netz versucht den Traffic zu beschnüffeln oder zusätzliche Inhalte in eine (nicht SSL-gesicherte) Weltnetzseite einzuschmuggeln. Bedingt durch das Prinzip des Onion Routings holt der letzte Node einer Kette die gewünschten Inhalte. Diese Inhalte liegen dem Node im Klartext vor, wenn sie nicht SSL- oder TLS-verschlüsselt wurden.

Durch einfaches Beschnüffeln wird die Anonymität des Nutzers nicht kompromittiert, es werden meist Inhalte mitgelesen, die im Weltnetz schon verfügbar sind. Nur wenn Login Credentials unverschlüsselt übertragen werden oder mman-in-the-middle Angriffeërfolgreich sind, können die Bad-Exit-Nodes an persönliche Informationen gelangen.

Persönliche Daten (bspw. Login Daten für einen eBrief- oder Bank-Account) sollten nur über SSL- oder TLS-gesicherte Verbindungen übertragen werden. Bei SSL-Fehlern sollte die Verbindung abgebrochen werden. Das gilt für anonymes Surfen via Tor genauso, wie im normalen Web.
Liste bekannter Tor-Bad-Exit-Nodes (unvollständig)

Die folgenden Nodes wurde dabei erwischt, den Exit Traffic zu modifizieren, z.B JavaScript in abgerufene Weltnetzseiten einzuschmuggeln. Dabei handelte es sich zumeist um Werbung oder Redirects auf andere Seiten. Name Fingerprint(s)

- CorryL 3163a22dc3849042f2416a785eaeebfeea10cc48
- tortila acc9d3a6f5ffcda67ff96efc579a001339422687
- whistlersmother e413c4ed688de25a4b69edf9be743f88a2d083be
- BlueMoon d51cf2e4e65fd58f2381c53ce3df67795df86fca
- TRHCourtney01 f7d6e31d8Af52fa0e7bb330bb5bba15f30bc8d48
- Unnamed 05842ce44d5d12cc9d9598f5583b12537dd7158a
- f36a9830dcf35944b8abb235da29a9bbded541bc
- 9ee320d0844b6563bef4ae7f715fe633f5ffdba5
- c59538ea8a4c053b82746a3920aa4f1916865756
- 0326d8412f874256536730e15f9bbda54c93738d
- 86b73eef87f3bf6e02193c6f502d68db7cd58128

Die genannten Nodes sind nicht mehr online, die Liste ist nur ein Beispiel.

Die folgenden Nodes wurden bei dem Versuch erwischt, SSL-Zertifikate zu fälschen, um den verschlüsselten Traffic mitlesen zu können:

- „LateNightZ“ war ein deutscher Tor-Node, der 2007 beim man-in-the-middle Anriff auf die SSL-Verschlüsselung erwischt wurde.
- „ling“ war ein chinesischer Tor-Node, der im Frühjahr 2008 versuchte, mit gefälschten SSL-Zertifikaten die Daten von Nutzern zu ermitteln. Gleichzeitig wurde in China eine modifizierte Version von Tor in Umlauf gebracht, die bevorzugt diesen Node nutzte. Die zeitliche Korrelation mit den Unruhen in Tibet ist sicher kein Zufall.
- Im Sept. 2012 wurden zwei russische Tor Nodes mit den IP-Adressen 46.30.42.153 und 46.30.42.154 beim SSL man-in-the-middle Angriff erwischt.
- Im April 2013 wurde der russische Tor-Node mit der IP-Adresse 176.99.10.92 beim SSL man-in-the-middle Angriff auf Wikipedia und auf IMAPS erwischt.

Im Februar/März 2012 haben mehrere Exit-Nodes in einer konzertierten Aktion die HTTPS-Links in Weltnetzseiten durch HTTP-Links ersetzt. Wie man damit erfolgreich die SSL-Verschlüsselung aushebeln kann, wurde auf der Black Hack 2009 demonstriert. Die Software für diesen Angriff heißt ssl-stripe und ist als Open Source verfügbar.

- Name Fingerprint und IP-Adresse
  Bradiex bcc93397b50c1ac75c94452954a5bcda01f47215 IP: 89.208.192.83

- TorRelay3A2FL ee25656d71db9a82c8efd8c4a99ddbec89f24a67 IP: 92.48.93.237

Tor-Exit-Nodes aus dem Iran sind generell als Bad-Exits markiert. Diese Nodes unterliegen der iranischen Zensur. Außerdem wird beim Aufruf von Weltnetzseiten über diese Nodes von der staatlichen Firewall ein unsichtbarer IFrame aus dem Hidden Internet of Iran eingefügt. ¡iframe src=„http://10.10.34.34“ style=„width: 100%; height: 100%“ scrolling=„no“ marginwidth=„0“ marginheight=„0“ frameborder=„0“ vspace=„0“ hspace=„0“¿ ¡/iframe¿
Es gibt seit Jahren eine andauernde Diskussion um die Tor-Exit-Nodes aus dem IP-Netz 149.9.0.0/16. Einige Leser haben mich öfters auf diese Nodes hingewiesen und vermuten, dass die NSA dahinter steckt:

- Name IP-Adresse
  busbyberkeley 149.9.0.60
  myrnaloy 149.9.0.59
  nixnix 149.9.0.58
  jalopy 149.9.0.57

Diese Tor-Server werden von Team CYMRU betrieben. TorProject.org sieht keine Veranlassung, diesem kommerziellen Privacy-Team zu misstrauen und die Nodes zu sperren. Das sind keine Bad-Exits.

7.7 Tor-Good-Exits

Im Abschnitt Tor-Bad-Exits sind einige Nodes genannt, denen man nicht trauen sollte. Diese Aufzählung kann nicht vollständig sein. Es ist so gut wie unmöglich, einen passiv schnüffelnden Tor-Node zu erkennen.

IT-Sicherheitsforscher haben mehrfach nachgewiesen, dass es recht einfach möglich ist, mit schnüffelnden Exits Informationen über die Nutzer zu sammeln (D. Egerstad 2007, C. Castelluccia 2010). Man kann davon ausgehen, dass verschiedene Organisationen mit unterschiedlichen Interessen im Tor-Netz nach Informationen phishen. Auch SSL-verschlüsselte Verbindungen sind nicht 100 Prozent geschützt. C. Soghoian und S. Stamm haben in einer wissenschaftlichen Arbeit gezeigt, dass

Geheimdienste wahrscheinlich in der Lage sind, gültige SSL-Zertifikate zu fälschen.

Als Verteidigung können Nutzer in der Tor-Konfiguration Exit-Nodes angeben, denen sie vertrauen und ausschließlich diese Nodes als Exit-Nodes nutzen. Welche Nodes vertrauenswürdig sind, muss jeder Nutzer selbst entscheiden. Die folgende kurze Liste soll Anregungen zum Nachdenken liefern.

- Torservers.net ist eine vertrauenswürdige Organisation, die mehrere Exit-Nodes betreibt.
- Die von der Swiss Privacy Foundation betriebenen Tor-Exit-Nodes sammeln keine Informationen.
- Der CCC betreibt nach eigenen Aussagen die vier Tor-Nodes: chaoscomputerclub42, chaoscomputerclub23 sind Exit-Nodes. (wird ergänzt, sobald verifiziert)
- Der Node FoeBud3 wird wirklich vom FoeBud betrieben.

Bei der Auswahl der Server sollte man nicht einfach nach dem Namen im TorStatus gehen. Jeder Administrator kann seinem Server einen beliebigen Namen geben und den Anschein einer vertrauensvollen Organisation erwecken. Die Identität des Betreibers sollte verifiziert werden, beispielsweise durch Veröffentlichung auf einer Weltnetzseite.
Konfiguration in der torrc.

In der Tor Konfigurationsdatei torrc kann man die gewünschten Nodes mit folgenden Optionen konfigurieren:

StrictExitNodes 1

ExitNodes

- $B15A74048934557FCDEA583A71E53EBD2414CAD9,
- $2DDAC53D4E7A556483ACE6859A57A63849F2C4F6,
- $B15A74048934557FCDEA583A71E53EBD2414CAD9,
- $6D3EE5088279027AD8F64FF61A079DC44E29E3DF,
- $9E9FAD3187C9911B71849E0E63F35C7CD41FAAA3,
- $FDBA46E69D2DFA3FE165EEB84325E90B0B29BF07,
- $FDFD125372A694F0477F0C4322E613516A44DF04

Die erste Option gibt an, dass nur die im folgenden gelisteten Nodes als Exit verwendet werden dürfen. Für die Liste der Exits nutzt man die Fingerprints der Nodes, beginnend mit einem Dollar-Zeichen. Die Fingerprints erhält man von verschiedenen TorStatus Seiten.

Konfiguration in Vidalia
Das Control Panel Vidalia bietet viele Möglichkeiten für die Konfiguration von Tor, aber nicht alle. Um Optionen zu konfigurieren, die nicht in Vidalia zugänglich sind, kann eine Konfigurationsdatei mit den zusätzlichen Optionen angegeben werden, die beim Start von Tor zu berücksichtigen sind. Unter Linux findet man diese Datei standardmäßig unter $HOME/.vidalia/torrc. Es kann jedoch eine beliebige andere Datei verwendet werden.
In die Tor-Konfigurationsdatei trägt man die oben genannten Optionen ein.

7.8 Tor-Onionland

Das Tor-Netzwerk ermöglicht nicht nur den anonymen Zugriff auf herkömmliche Angebote im Weltnetz sondern auch die Bereitstellung anonymer, zensurresistenter und schwer lokalisierbarer Angebote. Der Zugriff auf die sogenannten Tor-Hidden-Services ist nur über Tor möglich.

Eine kryptische Adresse mit der Top-Level Domain .onion dient gleichzeitig als Hashwert für ein System von Schlüsseln, welches sicherstellt, dass der Nutzer auch wirklich mit dem gewünschten Dienst verbunden wird. Die vollständige Anonymisierung des Datenverkehrs stellt sicher, dass auch die Betreiber der Angebote nur sehr schwer ermittelt werden können.

Es gibt mehere Angebote im normalen Weltnetz, die zusätzlich als Tor-Hidden-Service anonym und unbeobachtet erreichbar sind.

DuckDuckGo ist unter der Adresse http://3g2upl4pq6kufc4m.onion zu finden. Für Firefox gibt es bei Mycroft das Add-on DuckDuckGo (Tor) für die Suchleiste
Wikileaks gibt es unter http://isax7s5yooqgelbr.onion
EasyCoin.net ist eine Service zur anonymen Verwaltung einer Bitcoin Brieftasche und unter http://easycoinsayj7p5l.onion erreichbar

Meine „Sammlung“ an reinen Tor-Hidden-Services enthält im Moment (hiddenwiki.me):

34x Angebote, die kinderpornografischen Schmutz zum Download anbieten (teilweise ausschließlich und teilweise zusätzlich zu anderen Inhalten)
3x Angebote zum Thema „Rent a Killer“. Ein Auftragsmord kostet offenbar nur 20.000 Dollar (wenn diese Angebote echt sind)
Ein Angebot für gefälschte Ausweisdokumente (aufgrund der mit Photoshop o.ä. bearbeiteten Screenshots der Beispieldokumente auf der Weltnetzseite halte ich das Angebot selbst für einen Fake)
Mehrere Handelsplattformen für Drogen
Einige gähnend langweilige Diskussionsforen mit 2-3 Beiträgen pro Monat
Einige Index-Seiten mit Listen für verfügbare Hidden-Services wie das legendäre Hidden Wiki oder das neuere TorDirectory

In diesen Index Listen findet man massenweise Verweise auf Angebote mit Namen wie TorPedo, PedoVideoUpload, PedoImages. Nach Beobachtung von ANONYMOUS sollen 70 Prozent der Besucher des Hidden Wiki die Adult Section aufsuchen, wo dieses Schmutzzeug verlinkt ist.

Es gibt also kaum etwas, dass ich weiterempfehlen möchte. Vielleicht für unbeobachtete und vorratsdatenfreie Kommunikation die folgenden Dienste:

- TorMail: http://jhiwjjlqpyawmpjx.onion bietet SMTP und POP3. Es können auch eBriefe aus dem normalen Weltnetz unter xxx@tormail.net empfangen werden
- TorPM: http://4eiruntyxxbgfv7o.onion/pm/ bietet die Möglichkeit, Textnachrichten ohne Attachments unbeobachtet auszutauschen. Der Dienst erfordert das Anlegen eines Accounts. Das Schreiben und Lesen der Nachrichten erfolgt im Webinterface
- SimplePM: http://4v6veu7nsxklglnu.onion/SimplePM.php arbeitet komplett ohne Anmeldung. Beim Aufruf erhält man zwei Links: einen Link kann man als Kontakt-Adresse versenden, den zweiten Link für die InBox sollte man als Lesezeichen speichern. Es können einfache Textnachrichten via Webinterface geschrieben und gelesen werden
- Jabber-Server: für Instant-Messaging via XMPP:
  ch4an3siqc436soc.onion Port: 5222

ww7pd547vjnlhdmg.onion Port: 5222
3khgsei3bkgqvmqw.onion Port: 5222

- IRC-Server: p4fsi4ockecnea7l.onion Port: 6667 (Tor-Hidden-Service des Freenode Netzwerk, kann nur mit registrierten Nicks genutzt werden.)

Für die **Tor-Hidden-Services gibt es kein Vertrauens- oder Reputationsmodell. Es ist unbekannt, wer die Hidden-Services betreibt und es ist damit sehr einfach, einen Honeypot aufzusetzen.**

7.9 Kompatibilität verschiedener Weltnetzseiten mit Tor

Ich bekomme viele Hinweise auf Weltnetzseiten, die Tor nicht mögen, sich mit Tor nicht nutzen lassen oder Tor-Nodes explizit sperren. Wikipedia erlaubt keine anonymen Edits mit Tor, einige eBrief-Provider sperren Tor (z.B. Lavabit) oder weisen eBriefe als Spam ab, die via Tor verschickt wurden, Suchmaschinen sperren temporär immer mal wieder die Top-Exit-Nodes, Wordpress mag es nicht, wenn man via Tor Kommentare schreibt... Was kann passieren wenn eine Weltnetzseite die Tor-Exit-Server blockiert?
Teste es auf www.tor.s-f-n.org/proxy-blocker Einige Hinweise von Lesern kann ich verifizieren, andere sind scheinbar nur temporär oder betreffen nur einige High-Performance-Exits. Ich habe nicht vor, ständig einzelne Weltnetzseiten zu prüfen. Das Problem wird es immer geben und die Liste veraltet schneller, als ich tippen kann.

Wenn ein Webdienst Tor nicht mag, dann sucht man am besten eine Alternative. Das Weltnetz ist groß und es gibt für alles einen Ersatz, den man via Tor nutzen kann.

7.10 Das Tor-Netzwerk allein reicht nicht

Wenn du Tor nutzt, hast du schon Einiges für deine Anonymität im Weltnetz getan, nur das reicht noch nicht. Du kannst nämlich trotzdem noch durch Dritte identifiziert werden. Das liegt daran, dass es neben der IP-Adresse noch andere Möglichkeiten gibt, beim Surfen mehr über dich zu erfahren. Zur echten Verschleierung deiner Identität im Weltnetz gehört:

- der richtige Umgang mit Cookies
- der Schutz vor Spionage-Programmen (Spyware)
- eine Absicherung deines Computers
- Datenschutz in sozialen Netzwerken und Communities
- Schutz deines WLAN
- Hintergrundwissen über die staatliche Vorratsdatenspeicherung

Ohne diese Schutzvorkehrungen nutzt dir auch das Tor-Netzwerk nichts - Du bist unter Umständen weiter identifizierbar.

7.11 Weltnetz - Verläufe löschen

Sei es am Arbeitsplatz, zuhause oder bei einem Bekannten, für neugierige Zeitgenossen ist es leicht ersichtlich, welche Adressen du im Weltnetz aufgesucht hast; vorausgesetzt sie haben Zugriff auf den Computer, an dem du vorher durchs Web gesurft bist.

Sie müssen nur wissen, an welchen Stellen sie nachzuschauen haben. Vor allem der Verlauf (die History), der Cache (Pufferspeicher, temporäre Dateien) und die Cookies geben Aufschluss über deine Surfgewohnheiten. Vergessen solltest du natürlich auch nicht die sog. Bookmarks (Lesezeichen, Favoriten), falls du dort Adressen gespeichert hat, die nicht für fremde Augen bestimmt sind!

Natürlich ist es aber hier möglich diese Spuren zu verwischen. Das Programm cCleaner entfernt vor allem den Verlauf von besuchten Weltnetzseiten und diverse andere Verläufe, wie z.B. zuletzt benutzte Dateien oder eingegebene Suchbegriffe der Windows-Suche. Es ist auch möglich, unbenutzte und temporäre Dateien zu bereinigen.

Was wird vom cCleaner bereinigt?
Die Lösung: cCleaner

Mythen und Klischees in der Informatik zu beseitigen, erinnert nicht selten an den Kampf von Don Quijote, wobei der Unterhaltungswert in einigen arg strapazierten Bereichen eher gen null tendiert und sich auch eine gewisse Ermüdung breit macht, wenn es darum geht, ständig den gleichen Unsinn zu revidieren. Das soll uns nicht davon abhalten, noch einmal das Thema Datenmüll-Bereinigung und Registry Cleaner aufzugreifen, um vielleicht doch noch etwas mehr Skepsis bei dem Umgang mit diesen Tools zu erzeugen.

Um es ganz deutlich zu formulieren, in diesem Artikel geht es nicht um die Vorzüge von Registry Cleanern, sondern in erster Linie um den cCleaner, den wir nach wie vor für als sehr nützlichen Helfer beim Eliminieren von Datenmüll einstufen. Das Thema Registry Cleaner reflektieren wir in einem extra Kapitel gegen Ende dieser Anleitung, zu der wir dir viel Vergnügen und hoffentlich die richtigen Erkenntnisse wünschen...
Hier gezeigte Programmversion: v3.23.1823

Installation und wichtige Hinweise:

Um in den Genuß des cCleaners zu kommen, benötigst du natürlich den entsprechenden Download, eine 32 oder 64 bittige Unterscheidung gibts es weder für den Download noch für die Installation:

Nachdem du die Installationsdatei heruntergeladen hast, öffnest du sie mit einem Doppelklick. Achte bei der Installation bitte darauf, das du überflüssige Zusatzprogramme (speziell die Yahoo Toolbar oder Google Toolbar/Google Chrome) nicht mit installierst. Natürlich muß und will Piriform über dieses virale Marketing Geld verdienen, aber bitteschön nicht unbedingt gerade mit diesem Toolbar-Mist. Schließlich wollen wir die Datenmüllbeseitigung des cCleaners nicht dadurch konterkarieren, in dem wir quasi durch die Hintertür beispielsweise die Argusaugen des Suchmaschinen-Marktführers ins System zurückholen...

Während der Installation wirst du auch nach der Sprachversion gefragt, die du nach Gusto auswählen kannst, der cCleaner legt dir diesbezüglich kaum Steine in den Weg.

Auch die ganzen zusätzlichen Kontextmenüeinträge usw. sind absolut überflüssig (bitte den Screenshot beachten), weil sie nur zu Klicks verleiten, die eher an die Spontanität als Vernunft zu adressieren sind. Automatischen Updates sollte man grundsätzlich mit Skepsis gegenüberstehen, zumindest bei 3rd-party Software und zu denen gehört der cCleaner. Der Grund ist kausal, alles was in diesem Bereich aktiv ist, mischt sich in Systemressourcen ein, die nicht immer mit den hierarchischen Abfolgen eines Betriebssystems harmonieren!

Beim klick auf Fertig stellen ...

... öffnet sich ein Fenster in dem du gefragt wirst ob du nach nicht zu löschenden Cookies scannen möchtest. cCleaner möchte dir hier eine Hilfe sein und Coocies mit Passwortangaben nicht

löschen. Da du aber keine Passwörter oder Benutzernamen auf deinem Computer gespeichert haben möchtest klickst du hier auf NEIN.

Wichtige und gefahrlose Einstellungen:

Wenn die Installation absolviert wurde und du den cCleaner das erste mal mit Adminrechten startest, geht es an die Einstellungen des cCleaners, für die wir dir entsprechende Screenshots angefertigt haben, damit du die gefahrlosesten Einstellungen übernehmen kannst. Unsere Einstellungen basieren auf Langzeiterfahrungen mit den Betriebssystemen Windows XP -¿ Vista und Windows 7, wobei die aktuelle Windows 8 Preview sich bisher analog dazu verhält. Vista- und Windows 7 Benutzer starten den cCleaner immer mit Rechtsklick auf das Symbol und wählen „Als Administrator ausführen“.

Die Begründung für diese Einstellungen liegen auf der Hand: Kennwörter sollten grundsätzlich nie gespeichert werden, egal in welchem Bereich sie angelegt wurden. Verknüpfungen werden von Windows Vista und auch Windows 7 anders kategorisiert als noch zu Zeiten von Windows XP, darum raten wir von deren Bereinigung ab. Dies gilt ebenso für tiefergreifende Systembereinigungen (ausgegraute Bereiche), bei denen schon eine zu viel gelöschte Datei ausreicht, um die ersten Probleme zu generieren.

Was im Karteireiter „Anwendungen“ bereinigt werden kann, hängt natürlich in erster Linie davon ab, was du an externen Programmen installiert hast. Grundsätzlich sind diesbezüglich aber kaum Systemirritationen zu erwarten, zumindest nicht vom Betriebssystem. Darüber hinaus ist der cCleaner mittlerweilse so ausgereift, das diesbezüglich relativ wenig Substanz für Fehlerquellen existieren. Solltest du allerdings Software verwenden, die in dieser Hinsicht anfällig reagiert, kannst du jederzeit deren Optionshaken wieder entfernen.

Kurzum: Über diese nun klar definierte Reinigungsroutine kannst du deinen Computer gefahrlos z.B. nach jeder Internetsitzung oder Programminstallationen bereinigen, ohne das du sensible systemrelevante Bereiche tangiert. Selbstverständlich kannst du unsere Vorgabe auch nach Gusto ändern, wir haben so allerdings die besten Erfahrungen gemacht und unsere Prämisse hieß: möglichst gefahrlos und mit minimalem Risiko...!

apropos Risiko: Wir empfehlen ohnehin vor der ersten Systembereinigung mit dem cCleaner auf einem frisch eingerichteten System ein Image (Abbild) mit einer geeigneten Software zu erzeugen, damit du immer einen passenden Rettungsanker parat hast.

Den Karteireiter Registry ignorieren wir ganz bewußt (warum steht im separaten Kapitel) und widmen uns dem nächsten interessanten Punkt: der Button Extras:

Hier findest du insgesamt vier Untermenüs: Programme deinstallieren, Autostart, Systemwiederherstellung und Festplatten Wiper.

Programme lassen sich unter Windows Vista und Windows 7 mittlerweilse ausgezeichnet deinstallieren und falls nicht, hilft der cCleaner auch nicht entscheidend weiter, denn schlecht programmierte Deinstallationsroutinen lassen sich in der Regel von solchen Hilfsmaßnahmen wenig beeindrucken. Dies gilt ebenso für die Systemwiederherstellung, die ohnehin nur so gut funktioniert, wie Windows es zuläßt.

Festplatten Wiper (sicheres Löschen) von feierm Speicherplatz auf deinen Festplatten brauchst du eigentlich nicht solange du alle Daten sicher Löschst und nicht nur in den Papierkorb wirfst. Siehe: Dateien sicher löschen

Bliebe noch der Punkt Autostart, der in der Tat durchaus einige Ansätze bietet, um gezielt ins

System einzugreifen, wenn msconfig an seine Grenzen stößt:

Die Möglichkeit störende Einträge nicht gleich zu löschen, sondern zunächst zu deaktivieren und bei Bedarf wieder zu aktivieren, ist sicher einer der Vorzüge in diesem Abschnitt des cCleaners, zumal er neben dem Windows Autostart zusätzlich noch den Internet Explorer und Scheduled Tasks (geplante Aufgaben) als erweiterte Optionen anbietet, da kann msconfig nicht mithalten. Aber auch hier gilt wieder, Hände weg von der Maus, wenn du nicht weißt was diese oder jene Einstellung bewirkt und lösche bitte nicht gleich die Autostarteinträge ! sondern bleibe maximal bei der Deaktivierung.

Kommen wir zum Optionsbutton Einstellungen:

Unter Einstellungen -¿ Einstellungen achte bitte wieder darauf, dass du eine Optionen fürs sichere Löschen angehakt hast. Z.b.: Sicheres Löschen - Komplexes Überschreiben (7 Durchgänge).

Die Einstellungen der Cookies überlassen wir dir, diesbezüglich ist es kaum möglich, eine allgemeingültige Empfehlung abzubilden, dazu spielen in dieser Hinsicht zu viele verschiedene Faktoren eine Rolle. Wenn du aber der Meinung bist, das deine besuchten Weltnetzseiten keinerlei individuelle Surfgewohnheiten speichern sollten, kann die Konsequenz nur lauten: keine Ausnahmen in die Cookie Liste eintragen.

Willst du neben den standardmäßigen temporären Ordnern noch weitere bereinigen, so ist das über die Rubrik Benutzerdefiniert möglich. Eine Liste für mögliche temporäre Ordner (nicht alle sind auch zwangsweise vorhanden) unter Windows haben wir für kurz skizziert:

Windows XP:

C:/Windows/Temp/
C:/Dokumente und Einstellungen/Administrator/Lokale Einstellungen/Temp/
C:/Dokumente und Einstellungen/Default User/Lokale Einstellungen/Temp/
C:/Dokumente und Einstellungen/DeinBenutzername/Lokale Einstellungen/Temp/

Windows Vista/ Windows7:

C:/Windows/Temp/
C:/Benutzer/DeinBenutzername/AppData/Local/Temp/
C:/Benutzer/Default/AppData/Local/Temp/

Erfahrungsgemäß sammelt sich in den etwas versteckten Ordnern nur sehr wenig an, insofern sind die cCleaner Voreinstellungen normalerweise ausreichend. Wer es trotzdem ausprobieren möchte, kann die entsprechenden Temp-Ordner als benutzerdefinierte Ordner im cCleaner eintragen.

Bleiben noch zwei Einstellungs-Rubriken übrig, einmal die Option Auschließen, wo du Ordner ausschließen kannst, die nicht in die Bereinigung einfließen sollen. Unter Erweitert sind noch ein paar grundsätzliche Einstellungen möglich, die du aber nicht verändern musst.

Registry-Cleaner:

Wie versprochen greifen wir an dieser Stelle das leidige Thema Registry-Cleaner noch einmal auf. Es ist wahrlich erschreckend, wie arglos einige Anwender diese Tools einsetzen, obwohl sie deren Wirkung weder verifizieren noch sicher einschätzen können. Besonders ärgerlich wird es, wenn einige Windows Foren sich zwar gegen die Verwendung dererlei Tools aussprechen, im Gegenzug aber Adsense Werbung mit eben diesen Tools ins Forum stellen, das ist wirklich „konsequent“.

Um es auf den Punkt zu bringen, es existiert kein kausaler geschweige denn evidenzbasierter Beweis, das Registry Cleaner irgend etwas positives bewirken. Wenn ein solches Tool nach der Neuinstallation von Windows bei einer Analyse 700 zu optimierende Einträge findet, in der Masse sind das dann hauptsächlich Verweise auf nicht mehr vorhandene Dateien ¿ nicht mehr vorhandene Verknüpfungen und nicht mehr vorhandene Programme, sollten wirklich alle Alarmglocken klingeln, weil das entbehrt nun wirklich jeglicher Logik.

In diesem Zusammenahng von „Tuning“ zu sprechen ist ohnehin der blanke Hohn, aber es hält sich seit Jahren der Mythos, die Registry muss regelmäßig mit Hilfsprogrammen entschlackt werden, damit Windows optimal arbeitet. Dies ist de facto falsch, die Registry ist eine Datenbank, in der Windows und viele Programme entsprechende Konfigurationsdaten speichern.

Dort werden auch keinerlei ini-Dateien abgearbeitet sondern Datenbanken abgefragt, d.h. installierte Programme und Applikationen fragen ihre Keys und Einstellungen diesbezüglich bei Bedarf in den entsprechenden Hives ab. Das bedeutet im Klartext, dass nach einer Deinstallation des jeweiligen Programms diese Datenbankinformationen eben nicht mehr abgefragt werden, ergo haben sie auch keinen Einfluss mehr aufs System, ob sie nun da sind oder nicht.

Ebenso falsch ist die Behauptung, das die komplette Registry Datenbank permanent in den Arbeitsspeicher geladen wird und somit wertvollen Speicherplatz belegt und Windows so verlangsamt. Es wird definitiv nur das in den Speicher geladen, was verwendet wird: also die benötigten Hives, alles andere bleibt draußen, demzufolge kann die Registry niemals Windows verlangsamen. Ganz davon abgesehn, dass ein einziger übereifriger Löschvorgang in der Registry ausreicht, um eurer Betriebssstem entscheidend zu kompromittieren. Wenn dein Windows zu langsam ist, rüste deine Hardware auf, die Registry ist diesbezüglich der komplett falsche Ansprechpartner...

8 Computer

8.1 Betriebssystem - „Tails“

Frei und mit Anleitung herunterladbar unter **www.torproject.org**

Seit den „späteren“ Snowden-Veröffentlichungen vom März 2014 wissen wir leider mit Sicherheit, dass die Geheimdienste NSA, GCHQ und weitere für eine maßgeschneiderte Infiltration unserer Computer keine menschlichen Hacker mehr benötigen, sondern automatisiert mit dem Spionageprogramm Turbine1 unbemerkt spezifische Schnüffel-Software auf unseren Rechnern installieren.

Wir empfehlen angesichts dieser Angreifbarkeit über massenhaft infizierte Rechner, Tails als unveränderliches „Live-Betriebssystem“ für das Kommunizieren, die Recherche, das Bearbeiten und Veröffentlichen von sensiblen Dokumenten zu benutzen. Ein Live-Betriebssystem ist ein eigenständiges Betriebssystem, was von DVD oder USB-Stick gestartet werden kann, ohne es zu installieren. Euer Standard-Betriebssystem auf der Festplatte wird nicht angefasst

Tails hilft euch bei der Bearbeitung von sensiblen Text-, Grafik- und Tondokumenten. Tails verwendet beim Surfen, Mailen und Chatten automatisch die Anonymisierungssoftware „Tor“ und verändert zusätzlich die sogenannte „MAC-Adresse“ eurer Netzwerkkarte. Was das ist und wozu das von Nutzen ist, erklärt euch die Einführung dieser Anleitung.

Tails hinterlässt bei richtiger Nutzung keine Spuren auf dem Rechner - eure Festplatte bleibt unberührt. Ein eventuell (auf Betriebssystemebene) eingeschleuster Schadcode kann sich auf einer Live-DVD oder einem schreibgeschützten Live-USB-Stick als Start-Medium nicht „festsetzen“ und euch beim nächsten Rechnerstart nicht mehr behelligen.

Leitfaden folgt demnächst. Ihr könnt euch Tails auf **tails.boum.org** heruterladen.

8.2 Dateien löschen - Sind sie wirklich weg?

Dateien löschen ist schwieriger, als man glaubt. Denn wer Dateien auf der Festplatte nur in den Papierkorb schiebt oder durch einfaches Löschen entfernen will, wiegt sich in trügerischer Sicherheit. Scheinbar „gelöschte“ Dateien werden bei Windows-Systemen nämlich nicht wirklich entfernt. Wir verraten, wie du deine Dateien wirklich sicher löschen kannst.

Papierkorb heißt nicht gleich gelöscht

Stelle dir die Festplatte deines Computers vor wie ein Buch mit vielen Kapiteln und einem Inhaltsverzeichnis am Anfang. Wenn du nun Dateien in den Papierkorb schiebst oder einfach löschst, wird nur der Eintrag im Inhaltsverzeichnis gelöscht. Sprich: Der Eintrag im Inhaltsverzeichnis ist durchgestrichen, doch das Kapitel ist weiter vorhanden. So lange nämlich, bis es von einem weiteren Kapitel (also Dateien) überschrieben wird.

Zurück in der Computer-Technik bedeutet das, dass Windows den Speicherplatz gelöschter Dateien einfach nur als freigegeben markiert. Das Betriebssystem wird also darüber informiert, dass auf diesem Platz wieder neue Dateien gespeichert werden können. Wirklich verschwunden sind die alten Dateien aber nicht.

Hinzu kommt dabei, dass moderne Systeme in der Regel gleich mehrere Protokolle von aktuellen Speichervorgängen anfertigen, um im Falle eines Stromausfalls oder Systemfehlers die Dateien möglichst schnell wieder herstellen zu können. In der Praxis bedeutet auch das: Gelöscht ist nicht gleich gelöscht.

Gelöschte Dateien wiederherstellen

Spezielle Software und technische Verfahren machen es damit möglich, auch gelöschte Dateien der Festplatte wieder sichtbar zu machen. Experten können selbst die Inhalte einer formatierten oder defekten Festplatte rekonstruieren. Das ist gut, wenn man selbst auf diese wichtigen Dateien angewiesen ist, und sie somit noch retten kann. Die Kehrseite der Medaille ist sicherlich, dass sich so auch Unbefugte Zugriff auf sensible Inhalte (Korrespondenz, Bankverbindungen, Geschäftsbriefe o.ä.) verschaffen können.

Ein unrühmliches Beispiel dafür ist der Fall eines Websurfers, der bei einem Internetauktionshaus gebrauchte, aber vermeintlich gelöschte Festplatten ersteigerte. Es gelang ihm, die Dateien wiederherzustellen. Wie sich herausstellte, kam der Ersteigerer so in den Besitz höchst sensibler Polizeidateien - die Ermittler hatten schlichtweg auf die einfache Löschung ihrer Festplatten vertraut.

Und das ist kein Einzelfall. Software, um gelöschte Dateien wieder herzustellen, gibt es im Weltnetz sogar kostenlos. Damit ist es praktisch für Jedermann möglich, an Dateien zu kommen, die er eigentlich nicht zu Gesicht bekommen sollte.

8.3 Grundlagen: Speichern und Löschen von Daten

Bevor wir zum sicheren Löschen von Dateien auf deiner Festplatte kommen, solltest du wissen was Dateien überhaupt sind und wie sie auf deiner Festplatte gespeichert werden.

8.4 Wie werden Daten gespeichert

Bevor man Daten richtig löschen kann, muss man zunächst wissen, wo sich diese Daten überhaupt befinden. Denn oft ist es nicht nur die eigentliche Datei, die gelöscht werden muss.

Beim Kopieren, Verschieben und Komprimieren von Dateien bleibt die ursprüngliche Version der Datei erhalten. Mit Vorsicht sind auch sog. Versionierungssysteme zu genießen, bei denen explizit alte Versionen von Dateien aufgehoben werden, um sie später z.B. für Vergleiche und Wiederherstellungen zu nutzen. Insbesondere ist an dieser Stelle auf das Windows 2003 Server-Betriebssystem mit seinen neuen Schattenkopien hinzuweisen. Diese sollen den Benutzer vor dem versehentlichen Ändern oder Löschen von Dateien auf dem Server bewahren. Deshalb werden Änderungen an den Dateien in speziellen Speicherbereichen der Festplatte aufbewahrt, um so alte Versionen wiederherstellen zu können. Insofern ist auch hier das Löschen dieser (Schatten-)Dateien notwendig, um die Daten vollständig zu vernichten.

Aber auch Windows selbst erstellt Kopien der Daten: temporäre Dateien beinhalten Zwischenversionen der eigentlichen Datei und in der Auslagerungsdatei werden Speicherbereiche, die nicht mehr in den Hauptspeicher passen, aufbewahrt, um später wieder in den Hauptspeicher geladen zu werden. Temporäre Dateien werden zwar in der Regel beim Beenden des zugehörigen Programms gelöscht, aber auch hier ist das Löschen wieder nur das Freigeben des Speicherplatzes auf der Festplatte, so dass sich auch diese Daten rekonstruieren lassen.

8.5 Versteckte Datenspeicher

Daten verbergen sich aber auch noch an einigen anderen Stellen, auf die man als Benutzer normalerweise keinen Zugriff hat. Eines dieser Probleme stellen die sog. Cluster Tips dar. Jede Festplatte wird beim Formatieren in Zuordnungseinheiten (Blöcke) unterteilt. Sie sind die kleinste Einheit einer Festplatte, der von dem Betriebssystem verwendet werden kann. Bei den heutigen Größen von Festplatten im zweistelligen Terabyte-Bereich sind Zuordnungseinheiten mit einer Größe von 64 KByte keine Seltenheit mehr. Für das Betriebssystem bedeutet dies, dass selbst wenn eine Datei nur 12 KByte groß ist, sie dennoch einen Speicherbereich von 64 KByte belegt. Der Rest dieses Blocks bleibt ungenutzt.

Normalerweise ist dies nicht problematisch, aber Speicherbereiche werden ja auch wieder frei gegeben und mit anderen Daten überschrieben. Stellen wir uns nun vor, eine Datei hätte die Größe von 62 KByte und belegt damit einen Block. Diese Datei wird nun gelöscht, die Daten bleiben also erhalten, nur der Verzeichniseintrag verschwindet. In diesen Block wird nun eine neue Datei geschrieben. Diese sei für unser Beispiel nur 10 KByte groß. Somit werden auch nur die ersten 10 KByte des Blocks überschrieben, der Rest der alten Datei von immerhin 52 KByte bleibt erhalten. Dieses Beispiel lässt sich natürlich auf jede beliebige Datei übertragen, denn größere Dateien werden in Blöcke aufgeteilt, so dass der letzte Block in der Regel nicht vollständig belegt wird. Diese Datenfragmente werden als Cluster Tips bezeichnet. Das Problem hierbei ist, dass man an diese Fragmente nicht mehr herankommt, da der Block ja als zu einer existierenden Datei gehörig markiert ist. Nur mit Hilfe spezieller Löschprogramme können diese Bereiche gelöscht werden. Diese Verfahren werden als Wiping (Verwischen) bezeichnet.

8.6 Daten „zwischen den Zeilen“

Das Speichern der Daten auf einer Festplatte erfolgt durch die Magnetisierung kleinster Eisenpartikel, die entsprechend ihrer Ausrichtung den Wert 0 oder 1 liefern. Diese Partikel sind auf der Oberfläche der Platten aufgetragen und werden in Spuren unterteilt, so dass der Kopf der Festplatte die Daten lesen und schreiben kann. Daten werden aber nicht nur in der Hauptspur der Festplatte, sondern auch in deren Rändern geschrieben, d.h. diese Nebenspuren enthalten ebenfalls die Daten. Normalerweise ist dies nicht problematisch, da die Festplatte beim Lesen dieses

„Rauschen“ herausfiltert. Für den potentiellen Angreifer sind diese Nebenspuren jedoch geeignet, die Daten wiederherzustellen. Früher wurden hierzu einfache Verfahren wie eine minimale Dejustierung der Festplattenköpfe verwendet. Heutzutage sind diese Nebenspuren aufgrund der höheren Speicherdichte schwieriger zu erreichen. Dafür ist ein erheblicher technischer und finanzieller Aufwand und sehr detailliertes Wissen notwendig, so dass vermutlich nur sehr gut ausgestattete Datenrettungsunternehmen oder auch Geheimdienste dazu in der Lage sind.

8.7 Löschen von Daten

Löschen ist nicht gleich Löschen. So löscht beispielsweise das Verschieben von Dateien in den Windows-Papierkorb und dessen anschließende Leerung die Daten nicht wirklich von der Festplatte. Vielmehr wird nur der Verzeichniseintrag entfernt, die eigentlichen Daten bleiben weiterhin auf der Festplatte und können somit rekonstruiert werden. Auch das Formatieren von Partitionen und selbst eine Low-Level-Formatierung auf BIOS-Ebene sind keine sichere Löschung, da Daten - wenn auch mit mehr Aufwand - immer noch rekonstruiert werden können.

Ein- oder zweimaliges Überschreiben kann durch ein Fehlerfilter ausgeglichen werden und frühere Daten können wieder „zum Vorschein“ gebracht werden. Dabei bedient man sich des physikalischen Effekts, dass die Nullen und Einsen auf der Festplatte durch analoge Signale dargestellt werden. Diese entsprechen aber nie vollständig einer 0 oder 1, sondern werden durch Verrauschen zu 0,05 oder 1,05. Die Hardware gleicht diese Fehler durch Toleranzgrenzen aus, so dass eine 1 als 0,95 oder auch als 1,05 gespeichert sein kann. Aus diesen Schwankungen kann man mittels einer Mikroanalyse des analogen Datensignals und einer Differenz zum zugehörigen Digitalsignal Rückschlüsse auf die vorherigen Datenwerte ziehen. Denn wird eine 0 durch eine 0 überschrieben, so ergibt dies eine andere Feldstärke als wenn eine 0 durch eine 1 überschrieben wird. Dieses Verfahren ist zwar technisch aufwendig und auch nicht ganz billig, es zeigt aber, dass das bloße Überschreiben der Daten sie nicht auslöscht. Deshalb verwenden die gebräuchlichen Löschverfahren auch immer eine Kombination aus einem Datenwert und dessen Komplement, um das geschilderte Differenzverfahren unbrauchbar zu machen.

8.8 Dateien sicher löschen - durch Überschreiben

Eine echte Löschung aller Dateien auf der Festplatte kann man eigentlich nur durch den Einsatz eines starken Magnetfelds garantieren, das alle Informationen auf magnetischen Datenträgern zerstört.

Für den täglichen Einsatz ist dieses Prinzip aber natürlich völlig ungeeignet. Deshalb sollte man sich auf das „Entfernen durch Überschreiben“ konzentrieren. Das bedeutet, dass die zu löschenden Dateien auf dem Computer mit verschiedenen Zeichenfolgen beschrieben werden - und damit nicht mehr für die Rekonstruktion zur Verfügung stehen.

Die Dateien werden auf der Festplatte ja als Einsen und Nullen gespeichert. Man könnte nun denken, dass es ausreichen würde, all diese Binärzahlen z.B. mit Nullen zu überschreiben. Theoretisch würde es das auch. Unsere Festplatten funktionieren mit Magnetismus. Äusserst stark vereinfacht könnte man sagen: Magnetisch = 1; nicht magnetisch = 0. Würde man nun wie oben gesagt alles mit Nullen überschreiben, wäre jedoch immer noch ein gewisser Restmagnetismus übrig. Aus diesem Grund überschreibt man die Festplatte nicht nur einmal, sondern gleich mehrmals und dazu meist noch mit speziell ausgewählten Mustern.

Überschreibungsmethoden gibt es sehr viele, ich werde hier also nur kurz auf die gebräuchlichsten eingehen, die da wären:

Einfaches überschreiben:
Einmaliges überschreiben mit Nullen. Ziemlich unsicher, wenn Spezialisten an die Daten wollen,

aber wohl für von Normalpersonen bezahlbare Wiederherstellungsfirmen ausreichend.
RCMP TSSIT OPS-II:
„Royal Canadian Mounted Police Technical Security Standards for Information Technology in Appendix Ops-II: Media Sanitation“ überschreibt acht mal, ändert aber nur ein zufälliges Byte im überschreibmuster. auch nicht eben sicher.
US DoD 5220.22-M (8-306. / E):
Oft auch DoD short (kurzes DoD) genannt. Macht nur die Durchläufe 1, 2 und 7 der „vollständigen“ DoD-Methode. US DoD 5220.22-M (8-306. / E, C and E):
Die empfohlene Methode von Amerikanischen Department of Defense (Verteidigungsministerium). 7 Durchläufe lang und ziemlich sicher.
Gutmann: Diese Methode wurde von Peter Gutmann 1996 vorgeschlagen. Sie ist satte 35 Durchläufe lang und gilt als absolut sicher. Wie die einzelnen Schritte aussehen, kann man sich in der grossen Tabelle in der Mitte dieser Seite ansehen. Gutmann selbst sagt aber inzwischen, dass aufgrund von änderungen im Festplattenaufbau wenige Durchläufe mit Zufallswerten ausreichen würden (Siehe „Epilogue“ im gelinkten Artikel)

PRNG: Pseudo Random Number Generator. Diese Methode sieht einfach vor, die Dateien mehrfach mit Pseudo-Zufallszahlen („echte“ Zufallszahlen kann man am PC nicht erzeugen) zu überschreiben. Wieviel mal das getan werden soll, kann man normalerweise einstellen. Ich würde sagen, diese Methode (auf so ca. 3-5 Durchläufen) ist auch für Paranoiker wie mich super geeignet.

Die Frage, wie oft Dateien überschrieben werden müssen, damit sie wirklich nicht mehr wiederhergestellt werden können, ist umstritten. So empfiehlt das Bundesamt für Sicherheit in der Informationstechnik (BSI), Dateien mindestens dreimal zu überschreiben. Ähnlich sieht es die Navy Staff Office Publication vor. Das amerikanische Verteidigungsministerium empfiehlt das siebenfache Überschreiben sensibler Dateien (U.S. Department of Defense standards, US DoD 5220.22-M (8-306. / E, C and E)).

Als eine der sichersten Methoden des Überschreibens gilt die wie wir nun wissen die Gutmann-Methode. Wir empfehlen sehr sensible Daten mit der Gutmann-Methode zu löschen. Für den normalen Tagesgebrauch reicht aber US DoD 5220.22-M (8-306. / E, C and E) mit 7 Durchläufen durchaus aus.

Sensible Dateien auf der Festplatte:
Nicht nur im Papierkorb müssen sensible Dateien gelöscht werden. Rekonstruierbar sind derartige Dateien oft auch deshalb, weil sie sich an anderen Stellen auf dem Windows-System Hinweise auf sie finden lassen. Dazu zählt die Registry, die Windows-Auslagerungsdatei, und vor allem der unbenutzte, „freie“ Speicherplatz.

8.9 Eraser

Wer unerwünschte, unnötige oder sensible Dateien einfach nur in den Papierkorb seines Rechners verschiebt, macht einen Fehler. Denn wirklich gelöscht sind diese Dateien, wie du nun weisst, dann nicht.

Mit dem kostenlosen Löschprogramm Eraser lassen sich gezielt Dateien und freier Festplattenspeicherplatz unter Windows sicher löschen. Auch das sichere Überschreiben bestehender Festplattenpartitionen ist möglich. Neben dem direkten Löschen können auch Löschaufträge und Zeitpläne erstellt werden. Das quelloffene (Open Source) Eraser gehört zu den beliebtesten und bekanntesten Löschprogrammen.

Wie andere Löschprogramme auch, überschreibt Eraser den nach dem Löschen einer Datei frei gewordenen Bereich einer Festplatte mit neuen Daten. Je nach gewählter Löschmethode findet

die Überschreibung mit einem festgelegten Wert (z. B. nur Nullen), einem speziellen Muster oder einem zufälligen Muster statt. Durch das Überschreiben wird die Möglichkeit einer Rekonstruktion der ursprünglichen Daten verhindert. Beim gezielten Löschen von Dateien muss jedoch berücksichtigt werden, dass sich noch Kopien dieser Datei irgendwo auf der Festplatte befinden können.

Hier gezeigte Programmversion: 6.0.10.2620

Nachdem du die Installationsdatei heruntergeladen hast, öffnest du sie mit einem Doppelklick. Achte bitte darauf nur eine Stabile Version „Stable Builds“ herunter zu laden.

Bist du am Installationsfenster angekommen drückst du auf Next. Im nächsten Schritt musst du die Lizenzvereinbarungen akzeptieren und klickst weiter auf Next

Im ersten Fenster klickst du auf Complete. Next und im nächsten auf Install.

Ist die Installation beendet machst du einen Haken bei Run Eraser und klickst auf Finish

Jetzt siehst du das Hauptfenster (Erase Schedule) von Eraser. Die zu löschenden Dateien ziehst du einfach mit der Maus in das weiße Feld. Im Punkt Settings ist schon voreingestellt dass, die Dateien mit der Gutmann-Methode vernichtet werden. Wie du bereits weisst ist dies die beste aber auch langwierigste Methode seine Dateien sicher zu löschen.

Wenn du die zu löschenden Dateien in das Fenster ziehst, fragt das Programm noch einmal ob du die Datei wirklich vernichten möchtest. Bestätige dies mit Ja und wenige Zeit später ist die Datei unwiderruflich gelöscht.

Natürlich kannst du auch Dateien sicher löschen ohne das Programm immer öffnen zu müssen. Nach einem Rechtsklick auf die zu löschende Datei erscheint im Kontextmenü der Eintrag „Erase“. Die Dateien werden ohne Sicherheitsabfrage direkt gelöscht. Eine Benachrichtigung im Infobereich informiert kurz über den laufenden Löschvorgang und über den erfolgreichen Abschluss des Löschvorgangs.

Während des Löschvorgangs kann der Fortschritt unter „Erase Schedule“ eingesehen werden. Dieser Eintrag im Scheduler (Planer) wird bei erfolgreichem Abschluss gelöscht. Über die Option „Automatically remove tasks which run immediately and completed successfully“ kann dies geändert werden. Durch einen Rechtsklick auf den Eintrag im Scheduler kann die Logdatei aufgerufen werden (sofern Fehler aufgetreten sind, würden diese hier ohnehin angezeigt werden).

Dateien die sich schon im Papierkorb befinden löschst du sicher indem du mit der Maus auf den Papierkorb fährst und mit der rechten Taste das Kontexmenü öffnest. Hier kannst du die Option Eraser auswählen und auch entscheiden ob der Papierkorb sofort oder erst bei nächsten Hochfahren des Computers sicher entleert wird.

Mit der Funktion Erase unused space überschreibt Eraser den freien Festplattenplatz einer Festplatte bzw. Partition. Dadurch kann verhindert werden, dass zuvor „unsicher“ gelöschte Dateien wiederhergestellt werden könnten. Diese Funktion macht also in erster Linie Sinn, wenn du nicht die ganze Festplatte oder Partition löschen möchtest. Durch Erase unused space werden keine Dateien gelöscht oder gar das Betriebssystem beschädigt, es werden nur die ohnehin als frei markierte Festplattenbereiche überschrieben.

Dieser Vorgang kann je nach freier Kapazität der Partition und der gewählten Löschmethode sehr lange dauern. Die Festplatte wird dabei stark beansprucht und es ist empfehlenswert, während des Ausführens dieser Funktion die Festplatte nicht mit anderen Aktionen zu
belasten.

Der Eintrag Erase unused space erscheint im Kontextmenü, sobald ein Datenträger via Rechtsklick unter „Computer“ bzw. „Arbeitsplatz“ ausgewählt wurde.

Anmerkung:

Wir empfehlen dir, bei SD-Karten stets den kompletten leeren Speicher überschreiben zu lassen („Erase Unused Space“). Der komplette Speicher einer SD-Karte kann mindestens rund 100.000 Mal überschrieben werden. Eine verkürzte Lebensdauer der SD-Karte kann in Kauf genommen werden, zumal der technologische Fortschritt schneller vonstatten geht als der Verschleiß an Speichergeräten, sodass ein Speichergerät eher entsorgt wird, weil es obsolet ist, als dass es kaputt geht. Bezüglich Festplatten genügt das bloße Überschreiben brisanter Daten, **allerdings empfehlen wir generell eine komplette Festplatten-Verschlüsselung mit TrueCrypt bzw. VeraCrypt**, um einen Zugriff bereits im Versuch zu unterbinden.

8.10 Datenversand durch Windows verhindern

Microsofts Informations-Hunger ist enorm: Ohne uns zu informieren, überträgt Windows Daten an Microsoft. Beunruhigend daran ist, dass die Übertragung im Hintergrund abläuft und nur schwer zu ermitteln ist, was genau übertragen wird.

Dieses kleine und kostenlose Programm nimmt uns die Arbeit ab, mühsam nach den „bösen“ Einträgen in der Registry zu fahnden. Auch die nervenden automatischen Updates von einigen Programmen können, nach Rückfrage, abgestellt werden. Das hat nicht nur einen Sicherheitsaspekt, die Programme starten daraufhin schneller.

XPAntiSpy verhindert, dass Windows ungefragt persönliche Daten an Microsoft sendet.

8.11 Die Sache mit den Fotos - Exif-Anhang löschen

Wenn du eines im Zeitalter der Elektronik nie vergessen solltest, dann dies: Es gibt keine Privatsphäre mehr. Jedes elektronische Gerät, jede elektronisch übermittelte Nachricht, jedes elektronische Irgendwas verletzt dein Verständnis von Privatsphäre auf jede nur denkbare Weise, das gilt auch für ein scheinbar harmloses Ding - das Foto.

EXIF steht für Exchangeable Image File Format. Auf gut deutsch gesagt, werden mit diesem Format Metadaten in digitalen Bildern gespeichert.

Wenn das Bild mit einem Smartphone aufgenommen wird - was heutzutage bei sehr vielen Fotos der Fall ist, dann können die Regierung, aber auch ganz normale Leute (auch die, die dir gar nicht schaden wollen) mithilfe von Metadaten, die in dieses Foto eingebettet sind, das du soeben z.B. über Twitter verschickt oder bei Facebook gepostet hast, deine genauen Koordinaten ermitteln. Das heißt deinen Wohnort und den Ort von dem du das Foto gesendet oder gepostet hast.

Es ist egal ob Smartphone oder normale (digitale) Kamera, sie alle speichern überdies auch ihre Seriennummer, die Uhrzeit der Fotografie und andere Fakten ab. Vergleichbar ist das ganze mit dem Poststempel auf Briefen.

8.12 JPEG & PNG Stripper

Diese Exif Daten hinterlässt ein Samsung Smartphone auf deinem geschossenen Bild und selbst wenn du deine Bilder ins Weltnetz lädst bleiben diese Exif/Metadaten vollständig erhalten.

Und wieder freut sich der Staatsapparat, wenn er lustige Fotos von weißen Masken im Weltnetz sieht, die Metadaten ausliest und in deiner Wohnung erstaunlicherweise die gleiche Kamera findet, die ihren Stempel aufs Bild gedrückt hat. Dann ist guter Rat teuer. Einem solchen Szenario vorbeugen

Es gibt mehrere Möglichkeiten die Exif-Daten zu entfernen. Zum einen alle relevanten Informationen mit einem Hex-Editor zu löschen, aber wer macht sich schon diese Mühe. Deshalb gibt es ein kleines Programm namens „JPEG & PNG Stripper“. Es arbeitet extrem einfach und entfernt sämtliche Metadaten im Nu. Dabei bleibt die Qualität der Bilder unberührt.

Herunterladen kannst du das Programm unter: www.heise.de

Dieses kleine Programm funktioniert denkbar simpel, es überschreibt den kompletten Bereich in einem Bild, der eigentlich für die Metadaten bestimmt waren.

Eine Installation des Programms ist nicht notwendig - du kannst es mit einem Doppelklick sofort starten. In dem Fenster machst du Häkchen bei „Schreibschutz ignorieren“, „Zeige Verkleinerung“ und „Immer oben“. Die anderen Häkchen kannst du weg machen.

Jetzt kannst du ganze Ordner oder einzelne Bilder in das Fenster ziehen. Alles andere läuft vollautomatisch. Die Bilder werden direkt verarbeitet, also nicht kopiert oder ähnliches. Wichtige Bestandteile des Bildes werden nicht entfernt, sondern wie gesagt nur die verräterischen Anhängsel.

Die Bilder sind nun von den lästigen Metadaten befreit und du kannst sie ohne bedenken im Weltnetz verbreiten.

8.13 Die virtuelle Maschine

Virtualisierung ist ein Thema das oft auf unserem Netzwerk vorkommt und wir entschlossen dass die Zeit reif ist auf diesem Gebiet etwas zu schreiben. In der Vergangenheit stolperten unsere Nutzer mit dem Kopf vorraus in eine Technologie von der sie nichts oder nur wenig wissen und erhofften sich das beste. Virtuelle Maschinen, von jetzt an nur noch VMs genannt sind vielseitig in ihrer Benutzung und erlauben auf jedem Zugangslevel den PC in eine Test-Station oder ein isoliertes System mit nur wenig Klicks zu verwandeln. Was sie nicht tun werden ist ein perfektes sicheres System zu bieten, egal was man auch tut. Virtualisierung ist kein Sicherheits-Wundermittel. Ein schlecht Eingestelltes/Veraltetes Linux kann ebenso gehackt werden wie ein Windows oder Mac OS.

Die Prozedur um die Festplatte neu zu Partitionieren und einen Dualen Boot des primären OS und Linux zu erstellen kann schief gehen wenn ihr die Daten vorher nicht sichert, und somit einen kompletten Verlust der Daten auf dem Laufwerk zufolge haben. Oder anders Formuliert, es ist schwer etwas zu Googlen wenn eure Netzwerk Verbindungen nicht funktionieren und ihr dass System rebooten müsst um wieder online zu gehen und nachzusehen. Mit einer VM, könnt ihr Betriebssysteme installieren auf eurem momentanen System und es ausführen als wäre es ein eigenes System im Vollbildmodus. Das macht die Fehlersuche- und behebung zu einem Kinderspiel.

Ihr könnt sogut wie jedes Betriebssystem auf einer VM installieren, aber dieser Leitfaden wird nur die Installation von Linux Mint auf einem Windows Host zeigen. Dieser Leitfaden setzt vorraus dass eure CPU die Hardware Visualisierung unterstützt.

Die ruhende Kraft schlummert auch in Uralt-Computern die effizient dazu benutzt werden können mehrere Betriebssysteme auf Virtueller Hardware zur selben Zeit mit minimalen Leistungsanforderungen an den Host laufen zu lassen.

8.14 Echtzeitverschlüsselung von Dateien und Datenträgern

Die anonymen Entwickler des Verschlüsselungsprogramms TrueCrypt haben das Projekt abrupt eingestellt und warnen vor der Nutzung ihrer Software. Der Vorgang gibt Anlass zu vielen Spekulationen.

TrueCryt hat kleinere Schwachstellen, wie es fast jedes komplexe Programm hat, jedoch stehen diese einer Verwendung von TrueCrypt nicht entgegen. Zu diesem Ergebnis kam das Open Crypto Audit Project (OCAP) nach einer Analyse des Tools und des zugehörigen Quellcodes. Das Projekt hat ein umfangreiches Audit durchgeführt und nun den abschließenden Bericht dazu als PDF-Datei veröffentlicht.

Das heißt glücklicherweise für uns: Die letzte Version 7.1a des Verschlüsselungsprogramms TrueCrypt ist sicher und kann bedenkenlos weiter genutzt werden.

Der Fork VeraCrypt, der sich im Juni 2013 von TrueCrypt abspaltete, wird nach wie vor weiterentwickelt und behebt einige der bei dem Audit von TrueCrypt gefundenen Probleme. Im September 2015 wurde von einem Sicherheitsforscher eine Sicherheitslücke in TrueCrypt entdeckt, die beim Fork VeraCrypt behoben wurde.

VeraCrypt nutzt den original TrueCrypt Source-Code, deshalb passen die alten TrueCrypt Screenshots in dem Leitfaden auch zu VeraCrypt. Die aktuelle Version kann auf TrueCrypt-Container zugreifen sowie diese ins VeraCrypt-Format konvertieren. Weitere Informationen zum Thema TrueCrypt / VeraCrypt findest du im SfN Infoblog:
www.blog.s-f-n.org/tag/truecrypt
Gerade im Falle einer Hausdurchsuchung ist es von enormem Vorteil, wenn der gesamte Computer bzw. die gesamte Festplatte verschlüsselt ist. Mit dem Programm TrueCrypt ist dies zum Beispiel möglich. Man wird nach dem Start des Computers aufgefordert ein Passwort einzugeben und kann dann erst das Betriebssystem starten.

Ist der Computer ausgeschaltet, ist die komplette Festplatte mit einem bestimmten Algorithmus verschlüsselt und kann somit nicht von Behörden oder anderen Schnüfflern eingesehen werden. Desweiteren bietet eine Vollverschlüsselung Schutz bei eventuellem Diebstahl des Notebooks.

8.15 Verschlüsselungs- und Hash-Algorithmen von TrueCrypt

Das Programm arbeitet mit den Verschlüsselungsalgorithmen Advanced Encryption Standard (AES), Twofish sowie Serpent. Der Anwender hat die Wahl, einen einzelnen Algorithmus zu wählen oder die Algorithmen hintereinander zu kaskadieren (alle Reihenfolgen sind möglich). Alle drei Verschlüsselungsmethoden gelten aktuell als absolut sicher, wobei AES auch in vielen Ländern und bei den Militärs (z.B. USA) in der Kategorie „höchste Geheimhaltungsstufe“ zugelassen ist. Am sichersten erscheint uns die Kaskadierung aller drei Algorithmen.

Ferner stehen die Hash-Algorithmen SHA512, Whirlpool und RIPEMD-160, zum „Zerhacken“ der zu verschlüsselnden Daten und zum Generieren der Header-Keys, zur Verfügung. Wir bevorzugen RIPEMD-160 (bit), da zu diesem bisher keine Kollisionen gefunden wurden und er sehr perfomant arbeitet. Du kannst jedoch bedenkenlos den populären SHA512- oder den ebenso sicheren

Whirlpool-Hash-Algorithmus verwenden.

8.16 Unterstützte Systeme und Installation von TrueCrypt

Unterstützte Systeme
TrueCrypt unterstützt in der Version 7.1a die Windows-Systeme 7 und Vista (32/64-bit), XP (32/64-bit), W2K und Server 2003 und 2008 (32/64-bit) sowie Mac OS X 10.4 Tiger/10.5 und 10.6 (Snow) Leopard und Linux mit Kernel 2.4.x, 2.6.x (32/64-bit). Für Linux wurde seit Version 5.0 auch eine GUI (graphische Bedienoberfläche anstatt wie bisher ausschliesslich kommandozeilenbasiert) bereitgestellt.

Die Vollverschlüsselung von System-Partitionen ist allerdings nur unter Windows 7, -Vista, -XP, -Server 2003 und 2008 (jeweils 32/64-bit) möglich. Versteckte Betriebssysteme sind nur ab Version 6.0 unter Windows XP, -Vista oder -7 (jeweils 32/64-bit) zu haben. Installation von TrueCrypt

Hier gezeigte Programmversion: 7.1a

Zuerst lädst du dir die neuste Version von TrueCrypt herunter. Da es die Weltnetzseite der TrueCrypt Entwickler nicht mehr gibt lädst du dir die Datei vom s-f-n.org Server herunter. Alternativ kannst du dir VeraCrypt herunterladen

Nachdem du die Datei mit einem Doppelklick geöffnet hast musst du wie bei allen Programmen die Lizenzvereinbarung akzeptieren und drückst auf Accept, danach direkt auf Next.

Natürlich willst du das Programm auf dem Computer installieren und nicht nur entpacken. Du wählst also Install

In folgendem Fenster wird nun der Installationsort festgelegt sowie ein Wiederherstellungspunkt für Windows angelegt. Die Haken kannst du alle gesetzt lassen, wenn du jedoch weißt was du tust kannst du sie auch entfernen.

Nachdem du mit Install bestätigt hast beginnt die Installation.

Nach wenigen Sekunden siehst du dieses Fenster. Die Installation ist jetzt abgeschlossen und du bestätigst mit OK, danach sofort Finish.

In einem weiterem Fester wirst du gefragt ob du eine Hilfestellung für TrueCrypt benötigst. Wenn du weiterhin mit unserem Leitfaden arbeitest wird diese jedoch nicht benötigt.

8.17 Deutsche Sprache für TrueCrypt

Jetzt lädst du dir die Deutsche Sprachdatei herunter. Da es die Weltnetzseite der TrueCrypt Entwickler nicht mehr gibt lädst du dir die Datei vom s-f-n.org Server herunter.

Hast du die Datei auf deinem Computer öffnest du das .zip Archiv und extrahierst/kopierst die Datei Language.de.xml in den Ordner C:/Programme/TrueCrypt.

Nun kannst du das Programm über das Startmenü oder die Desktop-Verknüpfung starten. Es erscheint direkt die Frage ob du das Benutzerhandbuch lesen möchtest. Falls du der englischen Sprache mächtig bist und viel Zeit hast, kann du dies tun. In unserem Falle überspringst du aber diesen Punkt. Du hast nun das Hauptfenster in deutscher Ausgabe vor Augen.

8.18 Erstellen von Datentresoren

Die einfachste Möglichkeit seine privaten Daten zu verschlüsseln, ist die mittels eines Datentresors. Diese sogenannte Containerdatei wird beim Erstellen mit Zufallsdaten gefüllt und kann anhand des Passwortes in das System eingehängt werden. Dieser Tresor erscheint dann im Arbeitsplatz als neues Laufwerk. Du kannst ihn auch wie ein solches behandeln. Daten davon lesen, löschen, ihn mit neuen beschreiben – alles geschieht verschlüsselt in Echtzeit. Diese Tresore kann man entweder auf seiner Festplatte oder auf mobilen Datenträgern erstellen. Wunderbar eignet sich dafür natürlich die Verschlüsselung von USB-Speicherstiften.

Im Hauptfenster drückst du auf Volumen erstellen.

Hier wählst du „Eine verschlüsselte Containerdatei erstellen“ und drückst auf Weiter.

Nun wählst du Standart TrueCrypt-Volume und Weiter.

Im folgenden Fenster musst du nun den Speicherort sowie den Dateinamen des Tresors bestimmen.Weiter! Ersteinmal musst du auf dem Computer, wo auch immer du den Container haben möchtest, per Rechtsklick auf der Computer-Maus eine Datei erstellen. Der Name sowie die Dateiendung spielen hierbei überhaupt keine Rolle! Wir haben unsere Datei nun „tresor“ mit der Endung „.tc“ gatauft und in in das Verzeichnis des Laufwerk „D:/“ gelegt.

Als nächstes wird der Algorithmus ausgewählt, welcher die Grundlage der Verschlüsselung bieten soll. Am Besten wählst du den Advanced Encryption Standard (AES) oder Twofish. Diese bieten eine sichere Verschlüsselung bei wenig Systembelastung. Als Hash-Algorithmus kannst du RIPEMD-160 lassen.

Nun wählst du die Größe des Tresors, welche er am Ende haben soll. Diese richtet sich natürlich danach, was du alles darin speichern willst. Wenn es lediglich für ein paar Dokumente sein soll, reichen wenige Megabyte. Sollen jedoch ganze USB-Speicherstifte verschlüsselt werden, richtet sich die Größe nach der Stiftgröße. Ist er 1 Gigabyte groß empfiehlt es sich für rund 800 Megabyte zu wählen. Die restlichen 200 Megabyte dienen dem Programm TrueCrypt falls es ein Rechner, auf dem man den Tresor öffnen will, noch nicht installiert hat und andere Dateien, die nicht zwingendermaßen verschlüsselt werden müssen oder zum schnellen Dateiaustausch mit Freunden und Kameraden dienen.

Nun musst du ein Passwort wählen.
Bitte Abschnitt Das Passwort beachten!

Im folgenden Fenster wählst du das Dateisystem. Wenn du Daten die größer als 4 GB in deinem Datentresor lagern möchtest nimmst du NTFS ansonsten sollte FAT bleiben. Weiter geht's mit Formatieren. Den Mauszeiger in diesem Fenster zufällig hin und her bewegen. Je länger (min. 30 Sekunden) du die Maus bewegst, desto besser. Dies trägt zu einer verbesserten Verschlüsselung bei.

Nach einem Klick auf JA beginnt TrueCrypt seine Arbeit. Die Datei die du für TrueCrypt erstellt hast, in unserem Fall: „tresor.tc“, wird jetzt komplett Formatiert. TrueCrypt warnt dich in diesem Fenster noch einmal das diese Datei gelöscht und durch eine neue ersetzt wird.

TrueCrypt verschlüsselt jetzt deine Datei. Je nach Rechenleistung und größe der Datei kann das schon einige Minuten dauern.

Wenn die Verschlüsselung fertig ist bestätigst du die Meldung mit OK.

Jetzt wird noch einmal Weiter gedrückt und du bist wieder am Anfang. Falls du keinen weiteren

Tresor erstellen möchtest, drückst du auf Abbrechen.

Möchtest du diesen Tresor nun in dein System einbinden, wählst du ihn im Hauptfenster unter Datei aus, wählst oben einen Laufwerksbuchstaben und drückst auf Einbinden. Du gibst das Passwort ein und bestätigst mit OK.

Je nachdem welchen Laufwerksbuchstaben du gewählt hast, erscheint nun im Arbeitsplatz das neue Laufwerk, welches solange der Tresor ins System eingebunden ist, wie ein handelsüblicher USB-Speicherstift benutzt werden kann. Möchtest du den Tresor schließen drückst du im Hauptfenster auf Trennen.

8.19 Einzelne Festplatte Verschlüsseln

Du kannst mit TrueCrypt auch ganz einfach eine externe Festplatte oder einen Speicherstift komplett Verschlüsseln. Auch diese Speichermedien erscheinen dann im Arbeitsplatz als neues Laufwerk. Man kann sie auch wie eines behandeln. Daten davon lesen, löschen, ihn mit neuen beschreiben – alles geschieht verschlüsselt in Echtzeit.

Im Hauptfenster drücken wir auf Volumen erstellen.

Hier wählst du „Verschlüsselt eine Partition/ ein Laufwerk“ und drückst auf Weiter.

Nun wählst du Standart TrueCrypt-Volume und Weiter.

Im folgenden Fenster musst du nun den Speicherort bestimmen. Du suchst dir die externe Festplatte oder deinen Speicherstift und wählst ihn aus. Weiter!

Es folgt wieder eine Warnung von TrueCrypt, diese kannst du aber Ignorieren und mit einem Klick auf JA wieder schließen.

Es ist besser und sicherer das zu verschlüsselnde Laufwerk durch TrueCrypt formatieren zu lassen. Also nimmst du den ersten Punkt. Weiter!

Als nächstes wird der Algorithmus ausgewählt, welcher die Grundlage der Verschlüsselung bieten soll. Wähle am Besten den Advanced Encryption Standard (AES) oder Twofish. Diese bieten eine sichere Verschlüsselung bei wenig Systembelastung. Als Hash-Algorithmus kannst du RIPEMD-160 lassen. Weiter!

Die größe des Volumes kannst und musst du natürlich nicht ändern da du den Datenträger ja komplett Verschlüsseln willst. Weiter!

Nun musst du ein Passwort wählen.
Bitte Abschnitt Das Passwort beachten!

Weiter!

Im folgenden Fenster wählst du das Dateisystem. Wenn du Daten die größer als 4 GB auf deiner Festplatte lagern möchtest nimmst du JA ansonsten sollte NEIN angeklickt bleiben. Weiter

Im folgenden Fenster fährst du etwas mit der Maus im Fenster hin und her (um Zufallsdaten zu sammeln). Danach klickst du auf Formatieren. Den Mauszeiger in diesem Fenster zufällig hin und her bewegen. Je länger (min. 30 Sekunden) du die Maus bewegst, desto besser. Dies trägt zu einer

verbesserten Verschlüsselung bei.

Wenn die Verschlüsselung fertig ist bestätigst du die Meldung mit OK. Jetzt wird noch einmal Weiter gedrückt und du bist wieder am Anfang. Falls du kein weiteres Volumen erstellen möchtest, drückst du auf Abbrechen.

Möchtest du dieses Volumen nun in dein System einbinden, wählst du ihn im Hauptfenster unter Datenträger aus, wählst oben einen Laufwerksbuchstaben und drückst auf Einbinden. Dann gibst du das Passwort ein und bestätigst mit OK.

Je nachdem welchen Laufwerksbuchstaben du gewählt hast, erscheint nun im Arbeitsplatz das neue Laufwerk, welches solange die Platte/Stick ins System eingebunden ist, wie ein handelsüblicher USB-Speicherstift benutzt werden kann. Möchtest du das Volume schließen drückst du im Hauptfenster auf Trennen.

8.20 Verschlüsselung der „C:“ Festplatte (Systemfestplatte)

Wenn du deinen ganzen Computer verschlüsseln möchtest, d.h. die Systemfestplatte, dann bietet dir TrueCrypt auch dafür eine Möglichkeit. Dadurch ist das gesamte System geschützt und nicht nur einzelne Teile auf einer Festplatte.

Nach dem Verschlüsseln erscheint vor dem Hochfahren des Computers eine Passwortabfrage, ohne welche man keinen Zugriff auf gleichen erhält.

Im Hauptfenster drückst du auf Volumen erstellen.

Hier wählst du „System-Partition bzw. System-Laufwerk verschlüsseln“ und drückst auf Weiter.

Im folgenden Fenster wählst du Normal und bestätigst mit Weiter.

Wenn du deine Festplatte Partitioniert hast und den Punkt: Die Windows-System Partitionverschlüsseln nimmst wird nur die C:// Festplatte Verschlüsselt. Die Restlichen Partitionen musst du extra Verschlüsseln. Das Gesamte Laufwerk sollte aber nur verschlüsselt werden wenn sich auf der Festplatte keine andere durch TrueCrypt verschlüsselte Datei befindet da es sonst passieren könnte das du dir die schon vorhandene verschlüsselte Datei zerstörst! Hast du keine andere verschlüsselte Datei auf deiner Festplatte nimmst du am besten: Gesamtes Laufwerk verschlüsseln.

Hier kannst du wählen zwischen der Verschlüsselung einer Partition oder des Gesamten Laufwerks.

Da du im Regelfall nur ein Betriebssystem auf deinem Computer Installiert hast wählst du im folgenden Fenster Ein Betriebssystem aus uns bestätigst mit Weiter.

Als nächstes wird der Algorithmus ausgewählt, welcher die Grundlage der Verschlüsselung bieten soll. Am besten wählst du den Advanced Encryption Standard (AES) oder Twofish. Diese bieten eine sichere Verschlüsselung bei wenig Systembelastung. Als Hash-Algorithmus kannst du RIPEMD-160 lassen. Weiter!

Nun musst du ein Passwort wählen. Bitte Abschnitt Das Passwort beachten!

Im folgenden Fenster fährst du etwas mit der Maus im Fenster hin und her (um Zufallsdaten zu sammeln) und drückst anschließend auf Weiter. Den Mauszeiger in diesem Fenster zufällig hin und her bewegen. Je länger (min. 30 Sekunden) du die Maus bewegst, desto besser. Dies trägt zu einer

verbesserten Verschlüsselung bei.

Die Schlüssel wurden erfolgreich erstellt. Hier klickst du wieder auf Weiter.

Im folgenden Punkt musst du eine sogenannte Rettungs-CD (Rescue Disk) erstellen. Diese wird benötigt, falls der Boot-Loader (Programm welches direkt nach dem Hochfahren startet und das Passwort verlangt) oder das Betriebssystem defekt ist, oder von einem Virus befallen wurde. Diese CD ersetzt natürlich NICHT das sichere Passwort.

Du wählst einen Ort an dem das Abbild der CD gespeichert werden soll und bestätigst mit Weiter.

Dieses Abbild muss nun mit einem Brennprogramm, beispielsweise Nero (kommerziell) oder Img-Burn (kostenlos) gebrannt werden, um mit der TrueCrypt Verschlüsselung fortfahren zu können.

Du kannst solange nicht mit Weiter bestätigen, bis TrueCrypt die gebrannte Rettungs-CD im CD-Laufwerk erkennt. Nachdem du die CD gebrannt hast erhälst du die Meldung, dass die Rettungs-CD erfolgreich erkannt wurde. Jetzt kannst du mit Weiter fortfahren.

Bewahre die Rettungs-CD an einem Ort auf, wo diese vor Beschädigungen geschützt ist und Du sie im Notfall auch wieder findest!

Im folgenden Fenster werden dir nun verschiedene Sicherheitsstufen von Lösch-Methoden angeboten, durch welche die Daten auf der Festplatte sicher gelöscht werden können. Am besten wählst du 7-pass (US DoD 5220.22-M), um einen Kompromiss aus Sicherheit und Schnelligkeit zu erhalten. Weiter! Es erscheint nun eine Meldung, die dich davor warnt, dass diese Lösch-Methoden einige Zeit in Anspruch nehmen können, bestätige mit Ja. Es werden keine Daten auf der Festplatte gelöscht. Diese Löschung gilt nur dem Freien Speicherplatz!

Im nächsten Fenster teilt dir das Programm mit, dass es nun deinen Computer auf Kompatibilität testet und einige notwendige Veränderungen vornimmt. Drücke auf Test.

Drücke bei der Meldung, dass die Passwortabfrage nach dem Start des Computers nur in Englisch verfügbar ist, auf Ja. Nun noch zweimal auf Ja und der Computer startet neu. Du musst nun auch das erste Mal dein gewähltes Passwort eingeben, um das Betriebssystem starten zu können.

Hast du dein Passwort richtig eingegeben und dein Computer ist wieder hochgefahren, erhälst du die Meldung, dass der Test erfolgreich durchgeführt wurde. Du drückst nun auf Verschlüsseln.

Nach Bestätigen des aufgehenden Fensters mit OK beginnt das Programm deinen Computer zu verschlüsseln. Je nach Rechenleistung und Festplattengröße kann dieser Prozess etwas länger dauern, in der Regel jedoch mehrere Stunden. Für diese Anleitung haben wir die Festplatte nicht extra sicher Gelöscht. Du solltest auf jedenfall die Festplatte, wie oben beschrieben, mit 7-pass (US DoD 5220.22-M) löschen lassen

Hat TrueCrypt das Verschlüsseln deiner Festplatte beendet kannst du mit OK Bestätigen und auf Fertig stellen klicken.

Die Systemfestplatte ist nun vollständig verschlüsselt. Bei jedem Start des Rechners muss nun das gesetzte Passwort eingegeben werden.

Ab diesem Zeitpunkt werden jegliche Daten welche von der Festplatte gelesen oder auf sie geschrieben werden (Festplatte ¡-¿ Arbeitsspeicher) in Echtzeit mit dem gewählten Algorithmus kodiert. Nach dem Herunterfahren sind die Daten natürlich komplett verschlüsselt und für einen Nutzer ohne das gesetzte Passwort absolut unbrauchbar. Auch durch einen Ausbau der Festplatte und

Zugriff von Linux auf das Dateisystem kommt man nicht an die Daten heran

Optional: Das Boot-Menü anpassen

Wenn du nicht willst, dass jeder beim Hochfahren des Rechners sofort sehen kann, dass dieser mit TrueCrypt verschlüsselt ist, so lässt sich über Einstellungen -¿ Systemverschlüsselung die Passworteingabe beim Systemstart beeinflussen. Ein Haken bei Keine Texte im Pre-Boot ... sorgt dafür, dass beim nächsten Start lediglich ein schwarzer Bildschirm mit blinkendem Cursor erscheint. Weder im Verlauf der Passworteingabe, noch bei fehlerhaften Passwörtern erscheint irgendetwas auf dem Bildschirm. Erst beim richtigen Passwort und drücken der Eingabe-Taste fährt der Recher wie gewohnt hoch. Zudem kannst du im Feld darunter mit bis zu 24 Zeichen eine eigene Meldung festlegen, die bei der Passworteingabe erscheinen soll. Z.B. die von Truecrypt vorgeschlagene gefälschte Fehlermeldung „Missing Operating System“. Ansonsten verhält sich die Passworteingabe auch hier wie oben beschrieben.

8.21 Verschlüsselung der Festplatte mit verstecktem Betriebssystem

Seit Version 6.0 von TrueCrypt ist außerdem eine besondere Funktion integriert: Man hat nun die Möglichkeit, je nach Art des Passwortes welches man zu Beginn eingibt, entweder auf ein öffentliches oder ein verstecktes Betriebssystem zugreifen. Gibst du z.B. das Passwort sicher-1-HEIT-2-ist-3-WICHTIG, dein Notfallpasswort, ein, lädt der Computer dein öffentliches Windows, auf welchem du neben Firefox, Pidgin und einem Textverarbeitungsprogramm nichts weiter Bedenkliches gespeichert hast. Du kannst nun schnell dein privates ePostfach abrufen, deinem Kumpel Bescheid geben wann die Feier heute Abend steigt und schnell bei einem Auktionshaus auf das neue Mobiltelefon bieten, ohne dass ein potenzieller Angreifer merkt, dass du dich eigentlich gar nicht in deiner gewohnten Umgebung befindest. Es soll Fälle geben, in denen man gezwungen ist – oder wird – das Passwort herauszugeben, genau für einen solchen Fall wurde diese Funktion eingebaut. Bilst du nun alleine und in Sicherheit, gibst du dein anderes Passwort ein und es wird dein normales (geheimes) Windows, unter welchem du alle brisanten Daten und Konten gespeichert hast (so wenig wie möglich sensible Daten elektronisch hinterlegen - geht immer davon aus, dass es 100 prozentige Sicherheit nicht geben kann), hochgefahren. In dieser Umgebung kannst du nun in aller Ruhe deine Kontakte zu Kameraden pflegen, Projekte für die nächsten Aktionen planen und verwalten sowie interne Foren abrufen.

Soviel zum Allgemeinen, nun wird für die Interessierten die dahinterstehende Technik erläutert: Vor Installation des Betriebssystems wird die Festplatte in zwei Partitionen unterteilt, die erste dient dem öffentlichen Bereich, die zweite dem versteckten Bereich sowie versteckten Betriebssystem. Nachdem Windows und anschließend TrueCrypt installiert wurde, wird der versteckte Bereich, also die zweite Partition verschlüsselt. Ist die Verschlüsselung abgeschlossen, werden weniger brisante Daten, ein paar Fotos, Lieder und belanglose Textdokumente in diesen Bereich kopiert. Nun wird das auf Partition 1 befindliche Windows in Partition 2 versteckt eingebettet. Danach wird das auf Partition 1 befindliche Windows ebenfalls verschlüsselt. Wir haben nun drei Passwörter. Mit unserem ersten Passwort gelangen wir beim Hochfahren nach Eingabe desselbigen auf Partition 1, auf welcher das öffentliche Windows liegt. Anhand unseres zweiten Passworts können wir nun Partition 2 öffnen und sehen die belanglosen Daten, mehr nicht. Geben wir jedoch beim Hochfahren das dritte Passwort ein, wird das in Partition 2 eingebettete, versteckte Windows geladen. Voraussetzung für das Verschlüsseln der Festplatte mit dieser Methode ist, dass der vorhandene Datenträger in zwei Partitionen unterteilt ist. Dabei ist zu beachten, dass Partition 2, auf welche das versteckte Betriebssystem kommt, mindestens 5% größer sein muss als Partition 1. Diese sollte aber auch nicht viel größer sein, da die Größe des versteckten Betriebssystems immer nur so groß ist, wie die Größe von Partition 1. Haben wir also eine 160GB Festplatte und unterteilen diese in 30GB (Partition 1) und 130GB (Partition 2), so ist der Bereich auf Partition 2 in dem sich das versteckte Betriebssystem befindet am Ende auch nur maximal 30GB groß, d.h. uns gehen

abzüglich der 1GB an irrelevanten Daten auf Partition 2 rund 99GB verloren!

Im Hauptfenster drückst du auf Volumen erstellen.

Hier wählst du „System-Partition bzw. System-Laufwerk verschlüsseln“ und drückst auf Weiter.

Im folgenden Fenster wählst du Versteckt und bestätigst mit Weiter.

Es erscheint nun eine Meldung, die dir mitteilt, dass sich auf der momentanen Partition, auf der sich Windows befindet, keine sensiblen Daten befinden dürfen bzw. sollten. Bestätige dies mit OK und klicke dann auf Weiter.

Nun erscheint eine Warnung. Du musst dir bewußt sein das du eine Windows Installations CD/DVD benötigst um weiter machen zu können. Dies wird mit JA bestätigt.

Wieder erscheint eine Information die besagt das während des Verschlüsselungsprozesses auf keinen Fall in den Ruhezustand oder Standby-Modus gegangen werden solle (Deaktivieren!). Es wird wieder mit OK bestätigt.

Im folgenden Fenster wählst du Ein Betriebsystem aus uns bestätigst mit Weiter.

Es folgt eine weitere Warnung. Das Betriebssystem muss bei Windows aktiviert sein. Wenn dein derzeitiges Betriebssystem den Anforderungen entspricht bestätige mit JA.

In den nächsten Schritten wird das äußere TrueCrypt Volumen (Partition 2) erstellt. Im folgenden Fenster drücken wir direkt auf Weiter.

Als nächstes wird der Algorithmus ausgewählt, welcher die Grundlage der Verschlüsselung bieten soll. Am Besten wählst du den Advanced Encryption Standard (AES) oder Twofish. Diese bieten eine sichere Verschlüsselung bei wenig Systembelastung. Als Hash-Algorithmus kannst du RIPEMD-160 lassen. Weiter! Merke dir welchen Algorithmus du wählst denn du MUSST! ihn zwingend in den nächsten Schritten erneut auswählen

Im folgenden Fenster wird die Gesamtkapazität der Partition 2 angezeigt. Bestätige mit Weiter

Nun musst du ein Passwort wählen. Bitte Abschnitt Das Passwort beachten!

Hast du dieses eingegeben, bestätigst du wieder mit Weiter.

Im folgenden Fenster wählst du das Dateisystem. Wenn du Daten die größer als 4 GB auf deiner Festplatte lagern möchtest nimmst du JA ansonsten sollte NEIN angeklickt bleiben. Weiter Wie empfehlen dir auf NEIN zu klicken und somit das FAT Format zu wählen

Nun musst du etwas mit der Maus im Fenster hin und her fahren (um Zufallsdaten zu sammeln). Den Mauszeiger in diesem Fenster zufällig hin und her bewegen. Je länger (min. 30 Sekunden) du die Maus bewegst, desto besser. Dies trägt zu einer verbesserten Verschlüsselung bei.

Danach drückst du auf Formatieren.

TrueCrypt verschlüsselt nun Partition 2. Dieser Vorgang kann, je nach Leistung des vorhandenen Computers, sehr lange dauern.

Wenn die Partition vollständig verschlüsselt ist, wirst du aufgefordert schein-sensible Daten darauf zu speichern. Öffne über den Knopf das äußere Volume und kopiere Daten hinein, die zwar

vertraulich wirken, es aber in Wahrheit gar nicht sind. Am Besten ist eine Mischung aus Dokumenten, Video- und Audiodateien, sowie Bildern. Empfehlenswert ist es auch nicht gerade nur 100 Megabyte zu belegen, sondern schon das ein oder andere Gigabyte (wenn möglich) um nicht ganz so auffällig zu wirken. Hast du das getan, drücke auf Weiter Die Daten auf dieser Partition darfst du nach Abschluss dieses Leitfadens auf KEINEN FALL mehr verändern! Falls doch, ist ein Datenverlust oder gar eine Zerstörung des versteckten Windows die Folge.

Jetzt beginnt die Erstellung des versteckten Betriebssystems.

Nachdem du in dem oberen Fenster auf Weiter gedrückt hast erscheint die von uns weiter oben schon angekündigte Warnung. Merke dir unbedingt den Algorithmus den du verwendest da du ihn in exakt gleicher Form öfter brauchen wirst. Weiter gehts mit einem Klick auf OK.

Als nächstes wird der Algorithmus ausgewählt, welcher die Grundlage der Verschlüsselung bieten soll. Am Besten wählst du den Advanced Encryption Standard (AES) oder Twofish. Diese bieten eine sichere Verschlüsselung bei wenig Systembelastung. Als Hash-Algorithmus kannst du RIPEMD-160 lassen. Weiter!

Nun musst du wieder ein Passwort wählen. Das Passwort für dieses versteckte Betriebssystem muss sich erheblich von den anderen beiden Passwörtern unterscheiden (d.h. von dem Passwort für das äußere Volumen und von dem Passwort für das Köder-Betriebssystem).

Als Passwort gibst du nun das wichtigste in diesem Leitfaden ein, denn dieses verschafft dir den Zugriff auf den sensiblen Bereich. Von daher sollte es stärker bzw. länger sein als die beiden anderen Passwörter. Weiter mit einem Klick auf OK. Bitte Abschnitt Das Passwort beachten!

Hast du das sichere Passwort eingegeben, bestätigst du wieder mit Weiter.

Nun musst du etwas mit der Maus im Fenster hin und her fahren (um Zufallsdaten zu sammeln). Den Mauszeiger in diesem Fenster zufällig hin und her bewegen. Je länger (min. 30 Sekunden) du die Maus bewegst, desto besser. Dies trägt zu einer verbesserten Verschlüsselung bei.

Danach drückst du auf Formatieren.

Sobald die Aktion abgeschlossen ist erhälst du die Bestätigung dass das versteckte Betriebssystem erfolgreich erstellt wurde. Klicke auf Weiter um fortzufahren.

Im nächsten Fenster wirst du darüber informiert, dass nun das Windows von Partition 1 in den versteckten Bereich von Partition 2 kopiert (Geklont) wird.

Drücke bei der Meldung, dass die Passwortabfrage nach dem Start des Computers nur in Englisch verfügbar ist, auf Ja. Nun noch zweimal auf Ja und der Computer startet neu.

Der Computer startet nun neu und du siehst zum ersten Mal den installierten Boot-Loader. Sieht ganz unspektakulär aus und fordert dich lediglich auf, dein Passwort für das versteckte Windows einzugeben. Hast du das getan beginnt auch schon der Kopiervorgang.

Ist der Kopiervorgang abgeschlossen, musst du nun nocheinmal das Passwort für das versteckte Betriebssystem eingeben und schon landest du zurück im Windows. Es erscheint ein Fenster, welches dich informiert das dieses Betriebssystem schreibgeschützt eingebunden wurde und ein weiteres Fenster welches dich auffordert, nun das öffentliche Windows zu löschen.

Du drückst jetzt zwei mal auf Weiter und landest beim Fenster: Sicher Löschen. In diesem Fenster werden dir nun verschiedene Sicherheitsstufen von Lösch-Methoden angeboten, durch welche die

Daten auf der Festplatte sicher gelöscht werden können. Am besten wählst du 7-pass (US DoD 5220.22-M), um einen Kompromiss aus Sicherheit und Schnelligkeit zu erhalten. Weiter!

Es erscheint nun eine Meldung, die dich davor warnt, dass der gesamte Inhalt der Partition, auf der sich das Original Betriebssystem befindet, gelöscht wird. Bestätige dies mit JA. Im darauf folgenden Fenster fährst du etwas mit der Maus im Fenster hin und her (um Zufallsdaten zu sammeln) und drückst anschließend auf Fortsetzen. Den Mauszeiger in diesem Fenster zufällig hin und her bewegen. Je länger (min. 30 Sekunden) du die Maus bewegst, desto besser. Dies trägt zu einer verbesserten Verschlüsselung bei.

Nachdem TrueCrypt das Original Windows gelöscht hat folgt ein Hinweisfenster welches du mit OK wegklicken kannst. Um eine glaubhafte Leugnung (plausible deniability) zu erreichen, musst du jetzt ein Köder-System erstellen.

Dazu musst du aus Sicherheitsgründen erstmal deinen Computer ausschalten und ihn mehrere Minuten ausgeschaltet lassen (je länger, um so besser). Dies ist notwendig um den Speicher zu leeren der sensible Daten enthalten kann. Schalte dann den Computer wieder an, aber starte nicht vom versteckten System aus, sondern Boote von einer Original Windows Betriebssystem CD/DVD und installiere Windows auf der Partition dessen Inhalt gerade gelöscht wurde (das heißt auf der Partition (C://!) auf der das Originalsystem installiert war, dessen Klon das versteckte System ist). Wenn du das Köder-System installierst wird es nicht möglich sein das versteckte System zu starten weil der TrueCrypt Bootloader vom Windows Systeminstallationsprogramm gelöscht wird. Das ist normal und zu erwarten. Du kannst das versteckte System wieder starten sobald du das Köder-System verschlüsselt hast weil TrueCrypt dann automatisch den Bootloader wieder installiert hat.

Ist Windows neu Installiert startest du dieses ganz normal und Installierst TrueCrypt. Denke daran, dass das Köder-System niemals sensible Daten enthalten darf

Starte TrueCrypt und drücke im Hauptfenster auf Volumen erstellen.

Hier wählst du „System-Partition bzw. System-Laufwerk verschlüsseln“ und drückst auf Weiter.

Im folgenden Fenster wählst du Normal und bestätigst mit Weiter.

Da die zweite Partition schon verschlüsselt ist wählst du hier: Die Windows System-Partition verschlüsseln.

Falls nur das versteckte Betriebssystem und das Köder-System auf dem Computer installiert sind, wählst du nun „Ein Betriebssystem“ (wenn mehr als diese beiden Systeme au dem Computer installiert sind wählst du „Mehrere Betriebssysteme“). Klicke dann auf Weiter.

In diesem Schritt musst du den selben Verschlüsselungsalgorithmus und den selben Hash-Algorithmus auswählen, den du auch für die versteckte Partition verwendet hast. Andernfalls wirst du auf das versteckte System nicht mehr zugreifen können.

Das Köder-System und das versteckte System müssen gleich verschlüsselt sein. Der Grund dafür ist, dass das Köder-System und das versteckte System sich einen Bootloader teilen werden, was nur einen einzigen, vom Nutzer gewählten, Algorithmus unterstützt (für jeden Algorithmus gibt es eine Extraversion des TrueCrypt Bootloaders).

In diesem Schritt wählst du ein Passwort für das Köder-Betriebssystem. Dieses Passwort kannst du einem Gegner/Angreifer verraten wenn du dazu gezwungen wirst dein Pre-Boot Authentifikations-Passwort zu verraten (das andere Passwort, dass du verraten kannst ist das für das äußere Vo-

lumen). Die Existenz des dritten Passworts (das Pre-Boot Authentifikations-Passwort für das versteckte Betriebssystem) bleibt geheim. Bitte Abschnitt Das Passwort beachten!

Das Passwort, dass du für das Köder-System wählst muss sich erheblich von dem für das versteckte Volumen (das versteckte Betriebssystem) gewählten Passwort unterscheiden.

Weiter!

Im folgenden Fenster fährst du etwas mit der Maus im Fenster hin und her (um Zufallsdaten zu sammeln) und drückst anschließend auf Weiter. Den Mauszeiger in diesem Fenster zufällig hin und her bewegen. Je länger (min. 30 Sekunden) du die Maus bewegst, desto besser. Dies trägt zu einer verbesserten Verschlüsselung bei.

Die Schlüssel wurden erfolgreich erstellt. Hier klickst du wieder auf Weiter.

Im folgenden Punkt musst du eine sogenannte Rettungs-CD (Rescue Disk) erstellen. Diese wird benötigt, falls der Boot-Loader (Programm welches direkt nach dem Hochfahren startet und das Passwort verlangt) oder das Betriebssystem defekt ist, oder von einem Virus befallen wurde. Diese CD ersetzt natürlich NICHT das sichere Passwort.

Du wählst einen Ort an dem das Abbild der CD gespeichert werden soll und bestätigst mit Weiter.

Dieses Abbild muss nun mit einem Brennprogramm, beispielsweise Nero (kommerziell) oder ImgBurn (kostenlos) gebrannt werden, um mit der TrueCrypt Verschlüsselung fortfahren zu können.

Du kannst solange nicht mit Weiter bestätigen, bis TrueCrypt die gebrannte Rettungs-CD im CD-Laufwerk erkennt. Nachdem du die CD gebrannt hast erhälst du die Meldung, dass die Rettungs-CD erfolgreich erkannt wurde. Jetzt kannst du mit Weiter fortfahren.
Bewahre die Rettungs-CD an einem Ort auf, wo diese vor Beschädigungen geschützt ist und Du sie im Notfall auch wieder findest!

Im folgenden Fenster werden dir nun verschiedene Sicherheitsstufen von Lösch-Methoden angeboten, durch welche die Daten auf der Festplatte sicher gelöscht werden können. Am besten wählst du 7-pass (US DoD 5220.22-M), um einen Kompromiss aus Sicherheit und Schnelligkeit zu erhalten. Weiter! Es erscheint nun eine Meldung, die dich davor warnt, dass diese Lösch-Methoden einige Zeit in Anspruch nehmen können, bestätige mit Ja. Es werden keine Daten auf der Festplatte gelöscht. Diese Löschung gilt nur dem Freien Speicherplatz!

Im nächsten Fenster teilt dir das Programm mit, dass es nun deinen Computer auf Kompatibilität testet und einige notwendige Veränderungen vornimmt. Drücke auf Test.

Drücke bei der Meldung, dass die Passwortabfrage nach dem Start des Computers nur in Englisch verfügbar ist, auf Ja. Nun noch zweimal auf Ja und der Computer startet neu. Du musst nun auch das erste Mal dein gewähltes Passwort eingeben, um das Betriebssystem starten zu können.

Hast du dein Passwort richtig eingegeben und dein Computer ist wieder hochgefahren, erhälst du die Meldung, dass der Test erfolgreich durchgeführt wurde. Du drückst nun auf Verschlüsseln.
Nach Bestätigen des aufgehenden Fensters mit OK beginnt TrueCrypt den Computer zu verschlüsseln. Je nach Rechenleistung und Festplattengröße kann dieser Prozess etwas länger dauern, in der Regel jedoch mehrere Stunden. Für diese Anleitung haben wir die Festplatte nicht extra sicher Gelöscht. Du solltest auf jedenfall die Festplatte wie oben beschrieben mit 7-pass (US DoD 5220.22-M) löschen lassen

Hat TrueCrypt das Verschlüsseln deiner Festplatte beendet kannst du mit OK Bestätigen und auf Fertig stellen klicken.

Nachdem du das Köder-System verschlüsselt hast ist der gesamte Prozess ein verstecktes Betriebssystem zu erstellen abgeschlossen. Du kannst nun drei Passwörter nutzen:

1. Das Passwort für das äußere Volumen
2. Das Pre-Boot Authentifikations-Passwort für das versteckte Betriebssystem
3. Das Pre-Boot Authentifikations-Passwort für das Köder-System

Wenn du das versteckte Betriebssystem starten möchtest, musst du nur das Passwort für das versteckte Betriebssystem im TrueCrypt Bootloader-Bildschirm eingeben (dieser erscheint nachdem du deinen Computer einschaltest).

Wenn du das Köder-Betriebssystem starten möchtest, musst du nur das Passwort für das Köder-System im TrueCrypt Bootloader-Bildschirm eingeben. Das Passwort für das Köder-System kann an jede Person ausgegeben werden, die dich zwingt dein Pre-Boot Authentifikations-Passwort zu verraten. Die Existenz des versteckten Volumen (und des versteckten Betriebssystems) bleibt geheim.

Das dritte Passwort (für das äußere Volumen) kann ebenfalls an jede Person ausgegeben werden, die dich zwingt dein Passwort für die erste Partition hinter der Systempartition zu verraten, in dem sich sowohl das äußere Volumen als auch das versteckte Volumen (mit dem versteckten Betriebssystem) befinden. Die Existenz des versteckten Volumen (und des versteckten Betriebssystems) bleibt auch hier geheim.

Wenn du das Passwort für das Köder-System einer Person verraten musst und du gefragt wirst warum der ungenutzte Speicherplatz der (Köder-)Systempartition zufällige Daten enthält kannst du zum Beispiel folgendes Antworten:

Die Partition enthielt zuvor ein mit TrueCrypt verschlüsseltes System aber ich habe das Passwort vergessen (oder das System wurde beschädigt) und musste Windows neu installieren und wieder verschlüsseln.

Wenn alle Anweisungen befolgt werden und alle Vorkehrungen und Voraussetzungen im Abschnitt „Security Requirements and Precautions Pertaining to Hidden Volumen“ in der TrueCrypt Bedienungsanleitung erfüllt sind, wird es unmöglich sein zu beweisen, dass das versteckte Volumen und das versteckte Betriebssystem existieren. Dies trifft auch zu wenn das äußere Volumen eingebunden ist oder wenn das Köder-Betriebssystem entschlüsselt oder gestartet ist. Auch durch einen Ausbau der Festplatte und Zugriff von Linux auf das Dateisystem kommt man nicht an die Daten heran

Optional: Das Boot-Menü anpassen

Wenn du nicht willst, dass jeder beim Hochfahren des Rechners sofort sehen kann, dass dieser mit TrueCrypt verschlüsselt ist, so lässt sich über Einstellungen -¿ Systemverschlüsselung die Passworteingabe beim Systemstart beeinflussen. Ein Haken bei Keine Texte im Pre-Boot ... sorgt dafür, dass beim nächsten Start lediglich ein schwarzer Bildschirm mit blinkendem Cursor erscheint. Weder im Verlauf der Passworteingabe, noch bei fehlerhaften Passwörtern erscheint irgendetwas auf dem Bildschirm. Erst beim richtigen Passwort und drücken der Eingabe-Taste fährt der Recher wie gewohnt hoch. Zudem kannst du im Feld darunter mit bis zu 24 Zeichen eine eigene Meldung festlegen, die bei der Passworteingabe erscheinen soll. Z.B. die von Truecrypt vorgeschlagene

gefälschte Fehlermeldung „Missing Operating System“. Ansonsten verhält sich die Passworteingabe auch hier wie oben beschrieben.

8.22 TrueCrypt Traveller Disk erstellen

Um TrueCrypt beispielsweise auf einen USB-Speicherstift zu bekommen, d.h. von dort portabel ausführen zu können, um die, auf dem USB-Speicherstift oder anderen Datenträger gespeicherten Daten, welche wiederum in einem TrueCrypt-Volume gespeichert/verschlüsselt und geschützt sind, auch von jedem Computer unterwegs öffnen zu können, rufst du im Programm den Menüpunkt „Extras/Traveller Disk erstellen“ auf und gibst im erscheinenden Fenster den Pfad* zum USB-Speicherstift an und belässt die Autostart-Konfiguration auf „Keine Aktion“. Du kannst jedes beliebige Verzeichnis wählen und den Ordner „TrueCrypt“ dann vor dort auf den USB-Speicherstift oder anderen Datenträger (z.B. CD/DVD) verschieben oder kopieren.

Bestätige mit „Erstellen“.
Anmerkungen:

Du kannst TrueCrypt(.exe) auf deinem USB-Speicherstift unter dem Ordner „TrueCrypt“ finden und von dort auf einem beliebigem Windows-Computer starten. Verschlüsselte Daten legst du in einem normalen Volume (Container) mit evtl. beinhaltendem versteckten Volume auf dem USB-Speicherstift ins Stammverzeichnis oder Unterverzeichnis deiner Wahl ab und verfährst wie obig beschrieben, um die Daten auf dem jeweiligen Computer einzubinden.

Auch ist es so für IT-Nomaden möglich, ein komplettes Betriebssystem wie z.B. „Knoppix“ oder Anwendungen über die „PortableApps-Suite“ von einem USB-Speicherstift aus entschlüsselt zu starten (man hat seinen ganzen Kram dabei und der Computer sieht aus wie Zuhause). Alle Daten werden auf dem USB-Speicherstift verarbeitet (bis auf den RAM, Computer durchstarten!). Nach Trennung, liegen die (aktualisierten) Dateien einschl. der Betriebssystem- und Anwendungsdaten wieder sicher verschlüsselt auf dem USB-Speicherstift. Auf einem Fremdrechner werden zwar mit den empfohlenen Optionen alle Daten (eben bis auf den RAM) mit dem Trennen des Volume gelöscht. Aber um den Arbeitsspeicher (RAM) auch zu löschen, sollte der Computer neu gestartet werden! Alle Spuren sind jetzt vernichtet und deine Daten liegen wieder sicher verschlüsselt auf deinem USB-Speicherstift.

Wenngleich TrueCrypt rein gar nichts auf der Festplatte hinterlässt, kann es dich nicht vor möglichen Memory-Dumps (Protokoll des Arbeitsspeichers) schützen, die der Eigner oder Administrator des verwendeten Computers veranlasst hat. Auch nicht vor Verlaufsspeichern (Dateinamen) des verwendeten Betriebssystems, installierter Überwachungs-Software oder Viren & Co. (z.B. Speicherung von Tastatureingaben), die sich auf einem Fremdrechner befinden können. Deshalb sollte man sich schon sehr sicher sein, wo man Daten ver- oder entschüsselt.

Wenn du keine Rückschlüsse auf die Existenz verschlüsselter Daten auf deinen Computer-Festplatten aufkommen lassen möchtest, deinstalliere TrueCrypt auf deinem Computer und starte TrueCrypt fortan von deinem USB-Stick, um deine Container einzubinden.

Einen USB-Speicherstift komplett zu verschlüsseln (Vollverschlüsselung einer Partition), also nicht im Traveller Disk Modus in Verbindung mit file hosted Volumes zu betreiben, macht nur dann Sinn, wenn immer gewährleistet ist, dass man an ein installiertes TrueCrypt-Programm herankommt. Für den mobilen Einsatz also zu vernachlässigen, es sei den man hat einen zweiten USB-Speicherstift mit einem installierten Traveller-TrueCrypt dabei.

8.23 TrueCrypt Volume auf CDs und DVDs

Möchtest du verschlüsselte Container auf einer CD oder DVD speichern, solltest du das Volume zuerst auf deiner Festplatte erstellen und anschliessend die entsprechende (Container-)Datei auf CD/DVD brennen. Soll auch das Programm TrueCrypt in ausführbarer Form dabei sein, musst du eine TrueCrypt Traveller Disk erstellen und auf die CD/DVD brennen. Somit kannst du TrueCrypt künftig von dieser CD/DVD aus starten und damit mit jedem beliebigen Windows-Computer die danebenliegende Container-Datei oder ein auf anderem Medium platziertes TrueCrypt-Volume einbinden/entschlüsseln.

Anmerkungen:
Da Brennvorgänge aufgrund der unterschiedlichsten Faktoren des öfteren fehl schagen bzw. nicht fehlerfrei ablaufen, ist es möglich, dass das TrueCrypt-Volume auf CD/DVD korrupt ist und sich aus diesem Grund nicht mehr einbinden lässt. Deshalb solltest du, bevor du die Quelle des Gebrannten löschst, den Volume-Header der Original-Containerdatei (auf der Festplatte) sichern (im Menü zu finden unter Extras) und, ganz wichtig, das gebrannte Volume probeweise einbinden und prüfen, ob alles ok ist. Im positiven Fall sollte noch eine Kopie gezogen und auf einem anderen Medium gespeichert werden (CDs/DVDs können auch kaputt gehen).

Öffnest du ein TrueCrypt-Volume direkt von CD/DVD, kannst du aufgrund der fehlenden Schreibrechte keine Veränderungen innerhalb des Volume vornehmen (im Gegensatz zur besseren Wahl des USB-Speicherstiftes), sondern lediglich die verschlüsselten Inhalte betrachten, öffnen und Dateien aus dem Container herauskopieren. Vorsicht, dies wäre aber eine dauerhafte Entschlüsselung, sofern nicht in ein anderes verschlüsseltes Volume kopiert wird.

8.24 Volume-Optionen von TrueCrypt

Diese Einstellungen betreffen nur TrueCrypt-Volumes und haben keine Bedeutung bei einer Vollverschlüsselung einer ganzen (System-)Partition oder eines kompletten Laufwerks (Sonderfall: Verstecktes Betriebssystem). Die wichtigsten Optionen erscheinen uns die folgenden (über Einstellungen ¿ Voreinstellungen in der Menüleiste zu erreichen):

Es ist sinnvoll ein TrueCrypt-Volumen immer als Wechselmedium einzubinden, um Windows daran zu hindern, gelöschte Dateien in den Papierkorb zu verschieben und den Ordner: „System Volume Information“ anzulegen. Im Papierkorb würde die Datei entschlüsselt landen und müsste, vor endgültiger Löschung aus dem Papierkorb, digital-forensisch entsorgt werden, ansonsten könnte sie wieder hergestellt werden.

Weiterhin sollte das Automatische Trennen der virtuellen Laufwerke bei Benutzerabmeldung, Bildschirmschonerstart und Wechsel in den Energiesparmodus aktiviert sein sowie die Option das sich alle Explorerfenster des zu trennenden Volume schliessen.

Um ein verschlüsseltes Volume glaubhaft Leugnen zu können sollte der Zeitstempel (Timestamp) von Containerdateien beibehalten werden. Andernfalls sieht ein potenzieller Angreifer das die verdächtige Datei brandaktuell ist.

Zu guter letzt ist es natürlich äußerst Wichtig den Kennwort-Speicher des TrueCrypt-Treibers beim Beenden sicher löschen zu lassen. Dies passiert auch bei automatischer Trennung.

8.25 Risiken bei Verwendung des Dateisystems NTFS (Host) und der Funktion Defragmentieren

Teile oder Fragmente einer TrueCrypt-Container-Datei (file hosted Volume), die unter der Verwendung des Dateissystems NTFS (neigt sehr zum Fragmentieren) eingebunden wurde sowie generell beim Defragmentieren, können im freien Speicher des Host-Systems als Kopie verbleiben. Beispielsweise durch temporäre Dateiverschiebungen bei einer Defragmentierung. Das bedeutet zwar nicht, dass die Datei dadurch entschlüsselt wäre (TrueCrypt speichert nichts ausserhalb seines Containers auf dem Speichermedium) aber der Dateiheader wäre möglicherweise wieder herstellbar, was zu nachfolgender Gefahr führt:

Änderst du beispielsweise dein Container-Passwort, weil das alte nicht mehr geheim ist, könnte ein Angreifer mittels des wiederhergestellten alten Dateiheaders das Volumen, in Kenntnis des alten und verbrannten Passwort, öffnen.

Um dies zu vermeiden, sollte man folgendes beachten:

Um ganz sicher zu gehen bleibt nur die Verwendung eines device-hosted TrueCrypt-Volume (ganze Partition vollverschlüsselt) oder einer verschlüsselten Systempartition (ganze Partition vollverschlüsselt) anstatt eines TrueCrypt-Containers (file-hosted).

Als Alternative böte sich noch die Verwendung eines Containers innerhalb eines isolierten virtuellen Betriebssystems an, welches - nach Bearbeitung und Export des Containers - auf seinen Ursprungszustand zurückgesetzt wird (durch schlichtes Ersetzen der Virtual-Machine-Image-Datei). So sind jegliche Betriebssystemspuren (auch im Freispeicher der virtuellen Maschine) beseitigt.

Sicheres digital-forensisches Löschen von Freispeicher auf dem verwendeten NTFS-System. Vor allem nach Defragmentierung!. Am besten gar nicht erst Partitionen defragmentieren, in welchen sich verschlüsselte TrueCrypt-Volumes befinden (auch nicht in anderen Dateisystemen formatierte Partitionen) bzw. die Volumes vorher auf eine andere Partition verschieben.

Einen TrueCrypt-Container (wenn möglich) in einem sog. non-journaling Dateisystem speichern (z.B. FAT, FAT32); da solche nicht so sehr zum Fragmentieren neigen wie NTFS. Man kann eine FAT (32) Partition auch neben einer NTFS-formatierten Systempartition in das System einhängen, sofern man entsprechende Ressourcen hat.

Beim Betrieb von TrueCrypt auf einem fremden Rechner (z.B. über USB-Speicherstift, siehe Traveller Disk erstellen) sollte, neben anderen Gefahren, auch bei NTFS grösste Vorsicht geboten sein.

8.26 Verwendung von Keyfiles (Schlüsseldateien)

Wir haben bereits kennengelernt, wie wir mit TrueCrypt eine Festplatte / Partition verschlüsseln und einbinden, wie das ganze mit einem Container ausschaut und wie wir mit einem Hidden Volume arbeiten können. Als weitere Sicherungsmaßnahme wollen wir nun mal schauen, wie wir mit sog. Schlüsseldateien arbeiten können. Ein verschlüsselter Bereich, dem ein Schlüsseldatei zugefügt wurde kann nur mit dem Passwort nicht entschlüsselt und eingebunden werden. Zum Entschlüsseln benötigt der Benutzer Passwort und Schlüsseldatei

Du kannst also z.B. deine Schlüsseldatei auf einen USB-Speicherstift kopieren und diesen nur an deinen Computer anschliessen wenn du den TrueCrypt Container öffnen möchtest. Somit kannst sicher sein dass das Knacken deiner Verschlüsselung fast unmöglich wird.
Der Einsatz einer Schlüsseldatei beginnt schon beim Erstellen des Containers bzw. Datentresors.

Bei der Passworteingabe wird es nun spannend. Wir können dort die Option Schlüsseldateien verwenden ankreuzen und dann auf „Schlüsseldateien verwalten“ klicken.

Als Schlüsseldateien können nun beliebig (viele) Dateien benutzt werden, auch die Endungen der Dateien ist egal. Es kann auch ein Verzeichnis verwendet werden, hier werden dann automatisch alle Dateien im Verzeichnis zu Schlüsseldateien.

Uns reicht hier eine Datei - ein Bild Namens: „20140316_164130.jpg“. Dies haben wir nach einem Klick auf Dateien hinzufügen eingefügt. Ein Klick auf OK, und nach der Passwortauswahl gehts auf Weiter. Nun geht es ans Formatieren der Datentresordatei und schon ist das Volume erstellt - geschützt per Passwort und Schlüsseldatei.

Jetzt geht es ans Einbinden bzw. öffnen des Datentresors. Dazu gehst du ganz normal über das TrueCrypt-Hauptfenster, wählst deine Datei aus und klickst auf Einbinden. Hier gibst du das Passwort ein - und was passiert?

Keine Chance, nur mit Passwort allein kommst du nicht mehr an die verschlüsselten Daten ran. Bei der Passworteingabe kann man aber unten jedoch Schlüsseldateien verwenden wählen und dann auf „Schlüsseldateien verwenden“ klicken.

Im nächsten Feld dann wählst du deine zuvor ausgesuchtes Schlüsseldatei.

Was passiert nach 2-fachen OK nun? Der Datentresor ist normal eingebunden.

Und schon ist unsere Verschlüsselung wieder ein wenig sicherer geworden. Es ist auch möglich, unter dem Menüpunkt Schlüsseldateien im TrueCrypt-Hauptfenster verschlüsselten Bereiche neue, weitere Schlüseldateien hinzuzufügen oder auch zu löschen. Gehen die Schlüsseldateien verloren, sind auch die verschlüsselten Daten verloren.

TrueCrypt ist schon eine sehr feine Sache - von der einfachen Verschlüsselung ausgehend gibt es weitere Möglichkeiten, sensible Daten sicherer zu verwahren. Doch sollte man sich auch hier niemals auf ein „Wird schon gehen“ verlassen - ein regelmässiges Ändern des Passwortes sowie der Schlüsseldateien, damit bloß keine Routine einkehrt ist unabdingbar. Routine ist heutzutage eines der größten Sicherheitslecks.

8.27 Verwendungsmöglichkeit im Hinblick auf den Bundestrojaner

Im Hinblick auf den Bundestrojaner bietet sich die Verwendung von TrueCrypt auf einem Offline-Rechner an, d.h. einem Computer, der nicht mit der Aussenwelt verbunden ist (auch nicht mit seinem lokalen Netz: LAN), sondern neue (sensiblen) Daten grundsätzlich verschlüsselt und vielfach geprüft (Hashes) über einen USB-Speicherstift, externe Festplatte oder anderweitiges externes Medium empfängt. Ein zweiter, mit dem Weltnetz verbundener, Computer sollte sensible Daten ebenfalls verschlüsselt (z.B. per eBrief Verschlüsselung) und nur von vertrauenden Quellen von aussen empfangen, die erst, nach intensiver Prüfung (Hash), auf das externe Medium, zur Übertragung auf den Offline-Computer, exportiert werden. Erst auf dem sicheren Offline-Computer werden die Daten dann mittels TrueCrypt on-the-fly entschlüsselt und weiter verwendet. Somit könnte der, zur Übertragung von Daten dienende, Computer durchaus über das Weltnetz infiltriert worden sein aber dem Angreifer würde es nichts nützen, weil die Daten verschlüsselt durchgereicht werden und er keine Möglichkeit hat, auf den Offline-Computer zuzugreifen (weil isoliert).

Sprich zum Offline-Computer müsste eine heimliche (händische) Vor-Ort-Installation der Remote-Forensic-Software (RFS=Bundestrojaner) erfolgen, was wiederum mit einer zusätzlichen Vollverschlüsselung des Systempartition einfach zu verhindern wäre.

Hast du nur EINEN Computer zur Verfügung, bietet sich der Einsatz eines zusätzlich versteckten Systems oder virtuellen Maschine an.

So oder so ähnlich werden wohl auch Terroristen - in Verbindung mit Steganograpie und/oder eBrief Verschlüsselung, vorgehen und sich vor staatlichem Zugriff schützen, weshalb eine heimliche Online-Durchsuchung nur den unbedarften Anwender trifft und somit am vorgegeben Ziel der Terrorismusbekämpfung vorbeischiesst.

8.28 Hackerschutz („Firewall“)

Kaum ein Thema wird im Weltnetz so kontrovers diskutiert wie das Thema Firewalls. Für den Websurfer selbst bringen derart theoretische Diskussion allerdings überhaupt nichts. Du musst wissen, was eine Firewall ist, wie sie funktioniert, und wo sie wirklich nützt. Das erfährst du in diesem Kapitel.

Was ist eine Firewall?
Übersetzt man das englische Wort Firewall ins Deutsche, so versteht man darunter eigentlich eine Brandschutzwand, also eine spezielle Mauer, die das Übergreifen der Flammen von einem Gebäudeteil auf einen anderen verhindert.

In der Computerwelt ist eine Firewall eine Software- oder Hardwarelösung, die zwischen zwei Netzwerke geschaltet wird (etwa zwischen Computer und Weltnetz), und den Datenverkehr zwischen diesen beiden Netzwerken filtert. Man könnte sich eine Firewall also wie einen Pförtner vorstellen, der alle ankommenden und ausgehenden Daten einer Gesichtskontrolle unterzieht und anhand dessen entscheidet, wen er durchlässt und wen eben nicht.

Experten unterscheiden zwischen zwei Arten von Firewalls, den Personal Firewalls (PF) bzw. Desktop Firewalls, und den „echten“ Firewalls. Unter Ersteren versteht man Software-Lösungen, sprich Programme, unter Zweiteren ganze Konzepte zum Schutz eines Computers, Servers oder Netzwerks.

Wer kann Firewalls nutzen? Im Prinzip jeder. Dabei wird man sicherlich Unterschiede machen. Wer ein ganzes Netzwerk - etwa das einer Firma - absichern will, muss natürlich zu ganz anderen Mitteln greifen als der private „surfer“, der nur seinen eigenen Rechner vor unerwünschten Eindringlingen oder Spionage-Software schützen will. Lösungen gibt es für beide, wobei wir uns hier ganz auf den Schutz des privaten Nutzers konzentrieren wollen.

Wie kompliziert ist der Betrieb einer Firewall?
Wenn du tatsächlich durch eine Firewall geschützt sein willst kommst du nicht umhin, zumindest einige Grundbegriffe und -Regeln zu kennen. Denn tatsächlich muss eine Firewall auch im privaten Einsatz gepflegt und konfiguriert werden. Das nötige Grundwissen erhältst du auf den nächsten Seiten.

8.29 Firewall und offene Ports

Ein kurzer Ausflug in die Technik bleibt uns beim Thema Firewalls nicht erspart, nämlich das Thema „Ports“, die manchmal geschlossenen, oft aber auch geöffneten Türen zu deinem Computer.

Damit ein Programm überhaupt mit dem Weltnetz kommunizieren kann, muss es auf deinem Computer eine bestimmte Tür öffnen, einen so genannten „Port“. Das heißt übersetzt so viel wie

„Durchlass“, was die Sache schon ziemlich genau beschreibt. Insgesamt stehen 65535 verschiedene Türen zur Verfügung, die „well known ports“ von 0 bis 1023, die „registered ports“ von 1024 bis 49151 und die „dynamic“ und/oder „private ports“ von 49152 bis 65535. Über diese Ports erledigen das Betriebssystem und die einzelnen Programme ihre Aufgaben, senden und empfangen etwa Informationen.

Ports: Die offenen Fenster
Offene Ports stellen allerdings auch ein Risiko da. Wer sich mit der Technik auskennt, kann diese Lücken nämlich für Einbrüche in den Rechner nutzen, vor allem in Verbindung mit Trojanischen Pferden.

Ganz plastisch kannst du dir offene Ports wie offene Fenster in deinem Haus vorstellen. Einem Einbrecher gleich dringt ein Trojanisches Pferd durch das Fenster in dein Haus ein, sammelt dort den Hausrat (oder eben sensible Daten) ein, und reicht ihn seinem Komplizen eben wieder durch das Fenster hinaus. Generell gesagt stellen alle offenen Ports ab Port 1024 ein gewisses Risiko dar, weil sie von unerwünschten Eindringlingen genutzt werden können.

Genau da kommt die Firewall ins Spiel - die Mauer, die vor die offenen Fenster gestellt wird. Der Expertenstreit, ob diese Mauer die offenen Fenster nun einfach schließen soll, oder dem Einbrecher besser vortäuschen soll, dass es überhaupt keine Fenster gibt (das so genannte Stealth-Prinzip), ist einmal mehr eher sicherheitsphilosophischer Art.

Für dich als Anwender ist eine andere Frage wichtig: Nützt mir eine Firewall oder schadet sie eher?

Dies wird im nächsten Kapitel beleuchtet.

8.30 Was eine Firewall bringt - und was nicht

Wer sich im Weltnetz bewegt, ist grundsätzlich der Gefahr von Angriffen ausgesetzt. Das können echte und bösartige Attacken auf den Rechner sein, zumindest aber Zugriffsversuche auf persönliche und private Daten. Doch auch von der anderen Seite her, von innen, drohen Gefahren für deine Privatsphäre. Wie kann hier eine Firewall von Nutzen sein? Spyware, Phonehome-Programme und Script-Kiddies

Echte Cracker werden in aller Regel nur selten Angriffe auf Hobbysurfer unternehmen. Ausgeschlossen ist sicherlich auch dieses nicht, ebenso wenig die Versuche so genannter Script-Kiddies, aus falsch verstandenem Ehrgeiz oder schlichter Boshaftigkeit fremde Computer zum Absturz zu bringen.

Weitaus größer allerdings ist die Gefahr, zum Opfer krimineller Angreifer zu werden, die durch das Ausspähen sensibler Daten wie Kreditkartennummern oder Passworten durch so genannte Trojaner echten finanziellen Schaden anrichten können. Gleiches gilt für das Risiko, durch so genannte Spyware zum „gläsernen Surfer“ zu werden. Sowohl der Werbeindustrie als auch den Herstellern von Computer-Programmes liegt viel daran, möglichst alles über die Surfgewohnheiten ihrer (potenziellen) Kunden herauszufinden. Oft wird dieses Ziel durch Spyware erreicht - kleine Programme, die Daten eines Nutzers von diesem unbemerkt über das Weltnetz an Firmen weiterleiten. Programme, die regelmäßig an ihren Hersteller bestimmte - auch persönliche - Daten des Benutzers verschicken, nennt man auch Phonehome-Programme.

Kontrollieren und Blockieren
Genau hier kommt die Firewall ins Spiel. Eine richtig konfigurierte Firewall überprüft sämtliche Datenverbindungen, die über deinen Computer laufen, egal, ob diese nun von außen herein wollen oder von dir, dem Computer, heraus. Anhand spezieller Regeln entscheidet die Firewall, ob sie

den jeweiligen Datenverkehr zulassen will. Wenn nein, blockiert sie diese Verbindung.

Genau das stellt den Schutz dar, den eine Firewall bieten kann: Unerwünschte Verbindungen, egal, ob sie nun von außen nach innen oder von innen nach außen wollen, werden an dieser „Zugangskontrolle“ überwacht und gegebenenfalls blockiert.

Beispiel:
Versucht ein Krimineller, auf einen Trojaner zuzugreifen, der auf deinem Computer installiert wurde, dringt er nicht durch. Und andersherum. Versucht beispielsweise ein Trojanisches Pferd, persönliche Daten von deinem Computer zu seinem LLenkerßu schicken, scheitert auch dieser an der Firewall - sofern du dies entsprechend eingestellt hast. Nach diesem Prinzip kann eine Firewall erheblich zu mehr Sicherheit und Privatsphäre im Weltnetz beitragen.

Nützliche und unnütze Beigaben
Ein gutes (Desktop-)Firewallsystem soll in der Lage sein, Datenströme zu kontrollieren und gefährlichen Datenverkehr auszubremsen. Viele Anbieter von modernen Firewalls für Privatanwender belassen es nicht allein dabei. Vielmehr geben sie ihrer Firewall noch eine Reihe anderer Eigenschaften mit, etwa Kontrollmechanismen über den eBriefverkehr, Werbeblocker oder Funktionen, um aktive Inhalte auszuschalten. Viele dieser „Beigaben“ erfüllen durchaus ihren Zweck. Du als Endanwender solltest bei der Wahl einer Firewall allerdings nicht zu viel auf diese Sonderfunktionen geben. Wichtiger ist es, dass deine neue Firewall den Zweck erfüllt, für den sie angeschafft wurde. Dazu gehört, dass die Firewall einfach, aber sicher zu konfigurieren (einzustellen) ist. Diesem Punkt widmet sich unser nächstes Kapitel.

8.31 Probleme bei Firewalls

Wenn wir beim Bild des Pförtners bleiben, lässt sich auch die Problematik einer Firewall gut darstellen: Damit der Pförtner seine Aufgabe erfüllen kann, muss man ihm zuvor genau erklären, anhand welcher Kriterien er entscheiden soll, wen er denn nun durchlassen darf, und wen nicht.

Zurück in der Computerwelt stellt gerade diese Definition der „Durchlass-Kriterien“, in der Fachsprache „Ruleset“ genannt, für den Laien oft ein Problem dar. Zudem muss sichergestellt sein, dass tatsächlich alle Daten über die Firewall geleitet und dort gefiltert werden. Gibt es auch nur einen „Hintereingang“, ist die Firewall so gut wie nutzlos.
Und noch ein dritter Punkt muss klar sein: Es genügt nicht, dass der „Pförtner“ nur die am Computer ankommenden Daten überwacht. Er muss auch die Programme überwachen, die vom Computer aus ins Weltnetz hinaus wollen. Gelingt es nämlich einem Angreifer, ein entsprechendes Programm (etwa ein Trojanisches Pferd oder Spyware) auf dem Rechner zu platzieren, könnten private Daten sonst ungehindert ihren Weg ins Netz finden.

Die Kontrollinstanz auf deinem Computer
Die häufig geäußerte Feststellung von Computerexperten, dass Firewalls für private Nutzer eigentlich nutzlos seien, hat aufgrund der oben dargestellten Problematik seine Berechtigung. Sie mögen ernsthaft durchgeführte Angriffe auf den Rechner nicht in allen Fällen abwehren. Aber wer tatsächlich die kriminelle Energie aufbringt, eine kleine Firewall zu „knacken“, würde vermutlich auch vor einer großen und ausgereiften Brandschutzwand nicht Halt machen. Letztlich musst also du für dich selbst entscheiden, ob du dich für eine Desktop Firewall auf deinem Computer entscheidest. Zumindest als gewisse Kontrollinstanz zum Schutz vor Ausspähung durch Trojaner oder Phonehome-Programme kann eine Personal Firewall nämlich durchaus nützlich sein. Allein die Tatsache, dass du auf deinem Rechner eine Firewall laufen hast, wird dich niemals vor echten Angriffen - gleich welcher Art - schützen können. Denn eine Firewall ist immer nur so gut wie ihr Benutzer. Wer sich also tatsächlich mit einer Firewall absichern will, sollte zumindest die Grundbegriffe des Datenverkehrs im Weltnetz kennen.

Ab und an sollte man seine Firewall auf ihre Funktion überprüfen. Dazu kannst du so genannte Portscans nutzen.

8.32 Teste dein System per Portscan

Firewall-Tests sind wichtig um zu prüfen, ob dein Computer offen für Angriffe von außen ist. Mehrere Institutionen und Organisationen halten dazu im Weltnetz Testseiten bereit.

Was ist ein Portscan?
Jeder Computer, der mit dem Weltnetz verbunden ist, kann anderen Systemen gewisse Dienste anbieten. Dazu sind offene Ports nötig - die umgekehrt ein Sicherheitsrisiko darstellen können. Stelle dir Ports als Türen zweier benachbarter Häuser vor. Wenn du deine Möbel zu deinem Nachbarn bringen möchtest, müssen beide Türen geöffnet sein - eben, um die Möbel transportieren zu können. Wenn du deine Haustür allerdings unbeaufsichtigt offen lässt, könnte ein Einbrecher in dein Haus eindringen.

Zurück in der Computerwelt lässt sich das Türen-Beispiel übertragen. Offene Ports sind nötig, um zum Beispiel Daten übertragen zu können. Portscanner sind Software-Programme die überprüfen, welche Dienste von deinem Weltnetz-Rechner angeboten werden. Da jedem Dienst ein eigener Port zugewiesen ist, lässt sich somit darauf schließen, welche TCP- und UDP-Ports an deinem Rechner offen sind und welche nicht. Das Ergebnis wird dir anschließend angezeigt. So hast du die Möglichkeit, eventuelle Schwachstellen an deinem Computer oder in deiner Firewall zu schließen.

Wichtig dabei ist natürlich die Seriosität der jeweiligen Portscan-Angebote. Dir ist kaum mit einem Sicherheitscheck gedient, der anschließend vom Anbieter dazu missbraucht wird, auf deinen Rechner einzudringen. Seriöse und gute Portscans findest du unter anderem bei:

www.scan.sygate.com
www.heise.de/security/dienste/portscan
www.check.lfd.niedersachsen.de/start.php
www.browsercheck.pcwelt.de/de/firewall-check

Wenn du eine Firewall einsetzt, wird dir diese in regelmäßigen Abständen anzeigen, dass dein Rechner „Opfer“ eines fremden Portscans geworden ist. Das bedeutet nichts anderes, als dass jemand deinen Rechner auf die von ihm angebotenen Dienste untersucht hat. Ein solcher Portscan kann zwar rein theoretisch der Anlauf eines Angriffs sein; in aller Regel ist er aber kein Grund zur Sorge. Du kannst einen Portscan mit einem Menschen vergleichen, der auf einem Parkplatz vor Auto zu Auto läuft und ausprobiert, ob irgendwo eine Tür offen ist. Vermutlich versucht dieser Mensch tatsächlich, in ein fremdes Auto einzubrechen. Doch wer seine Türen versperrt hat, hat vor diesem Menschen nichts zu befürchten. Und dazu gehörst ja auch du - oder?

8.33 Comodo Firewall

Vor der Installation der Firewall ist es am besten das du zuerst sicherstellst, dass dein Computer bereits frei von Malware ist. Hast du deinen Computer mit einem Anti-Virusprogramm durchgecheckt, deaktivierst du die Windows Firewall falls nicht bereits geschehen. Diese findest du in der Systemsteuerung oder der Startmenüsuche. Falls du bereits eine andere Firewall auf dem Computer hast, deaktiviere auch diese, die Comodo Firewall ist eine der besten und dazu noch komplett gratis!

Hier gezeigte Programmversion: 6.3.294583.2937

Zuerst lädst du dir die neueste Version von Comodo Firewall herunter.

Es wird unterschieden zwischen 32 und 64 Bit Systemen. Wenn du nicht weißt welches System du benutzt lädst du dir die 32 / 64 Version runter.

Die Installation Startet mit einem Doppelklick auf die Datei. Die Datei wird entpackt und du wählst natürlich Deutsch als Sprache aus. Weiter mit OK

Du hast nun die Wahl, Comodo möchte deinen, im Netzbetrachter eingestellten, DNS Server ändern. Dadurch werden Weltnetzseiten die Comodo als „gefährlich“ einstuft automatisch geblockt. Dies können also alle Seiten sein die Comodo gemeldet wurden.

(Wie du ordentliche DNS-Server einrichtest erfährst du auf den Seiten des Chaos Computer Club.)

In diesem Fenster machst du aber alle Haken raus und die eBrief Adresse wird natürlich auch nicht angegeben. Weiter gehts mit einem Klick auf Installation anpassen

In dem sich öffnenden Fenster machst du die Haken bei „Installiere Comodo Geek Buddy“ sowie „Installiere Comodo Dragon Web Browser“ raus, da wir ja nur die Firewall installieren wollen. Weiter gehts mit einem Klick auf Zurück und dann auf Weiter.

Nun möchte Comodo einen AdBlocker installieren. Dies ist unnötig da wir in unserem Firefox bereits das Add-On AdBlock Plus installiert haben. Also, Zustimmen und Installieren.

Die Installation beginnt.

Nach der Installation bittet dich Comodo deinen Computer neu zu starten. Dies tust du.

Ist dein Computer wieder hochgefahren hast du in der Mitte des Bildschirms ein Werbefenster welches du mit einem Haken, links unten nicht mehr auftauchen lassen kannst.
Du hast (meist in der rechten, oberen Ecke) ein neues Fenster welches dir anzeigt ob dein Computer sicher oder unsicher ist. Du kannst über dieses Fenster weiterhin deine installierten Netzbetrachter sicher, über eine Sandbox starten sowie das Controll Panel Comodos öffnen. Die Twitter und Facebook Buttons leiten dich auf die jeweiligen Seiten von Comodo, sind also für unsere Sicherheit nicht erwähnenswert.

Im Controll Panel Comodos siehst du nocheinmal ob dein Computer sicher ist und welche Programme z.Zt. in einer Sandbox ausgeführt werden.

Firewall grob einrichten

Die Firewall kann unterschiedlich eingerichtet werden. Ich bevorzuge die manuelle Methode, unter Comodo „Eigene Richtlinie“ bzw. „Custom Ruleset“, d.h. jedes Programm was ins Weltnetz möchte muss man selbst zulassen. Das ist am Anfang vielleicht etwas Arbeit, wird aber später immer weniger Aufwand und es hat den Vorteil, dass man sich mit den ganzen Windowsdiensten die vorher im Hintergrund ins Netz gekrochen sind beschäftigen muss, um zu wissen was man zulassen darf und was nicht.

Im Hauptfenster findest du rechts oben einen Pfeil, der dich zu den „Aufgaben“ führt.

Dort ganz unten klickst du auf den Reiter „Erweiterte Einstellungen“ und „Erweiterte Einstellungen öffnen“.

Dort wählst du in der Kategorie „Einstellungen zur Sicherheit“ „Firewall“ aus, wo du in den Firewalleinstellungen ganz oben den Modus auswählen kannst. Hier wählst du „Eigene Richtlinie“äus. Den Modus kannst du auch mit einem Rechtsklick auf das Comodo Trayicon unter „Firewall“

wechseln.

Die grobe Einrichtung ist nun abgeschlossen.

Versucht nun ein Programm zugang zum Weltnetz zu erlangen oder es möchte andere Dateien auf deinem Computer verändern wirst du in einem Pop-Up-Fenster gefragt ob du dies Erlauben möchtest oder nicht. Diese von dir gegebene Antwort merkt sich Comodo.

8.34 Die Comodo Firewall und OpenVPN

In dieser Anleitung zeigen wir dir, wie du OpenVPN mit der Comodo Firewall gegen sog. Leaks (offenlegungen) deiner richtigen IP-Adresse absicherst. Es sollte nicht schaden, wenn du dir die Comodo Firewall einmal herunterlädst und die verschiedenen Funktionen Schritt für Schritt kennenlernst, bevor du dich an die Anleitung wagst. Mit einer Desktopfirewall kann man zwar viel gutes machen, aber ebensoviel schlechtes was deiner Sicherheit im Weltnetz schaden kann. Diese Methode mit der Comodo Firewall unterscheidet sich von den anderen in dem Punkt, dass man die handvoll Regeln nur ein einziges Mal global erstellt und nicht für jedes Programm immer neue Regeln erstellen muss! Das dient der Übersicht und macht viel weniger Arbeit!

Firewall grob einrichten
Die Firewall kann unterschiedlich eingerichtet werden. Ich bevorzuge die manuelle Methode, unter Comodo „Eigene Richtlinie" bzw. „Custom Ruleset", d.h. jedes Programm was ins Weltnetz möchte muss man selbst zulassen. Das ist am Anfang vielleicht etwas Arbeit, wird aber später immer weniger Aufwand und es hat den Vorteil, dass man sich mit den ganzen Windowsdiensten die vorher im Hintergrund ins Netz gekrochen sind beschäftigen muss, um zu wissen was man zulassen darf und was nicht.

Im Hauptfenster findest du rechts oben einen Pfeil, der dich zu den „Aufgaben" führt.

Dort ganz unten klickst du auf den Reiter „Erweiterte Einstellungen" und „Erweiterte Einstellungen öffnen".

Dort wählst du in der Kategorie „Einstellungen zur Sicherheit" „Firewall" aus, wo du in den Firewalleinstellungen ganz oben den Modus auswählen kannst. Hier wählst du „Eigene Richtlinie" aus. Den Modus kannst du auch mit einem Rechtsklick auf das Comodo Trayicon unter „Firewall" wechseln.

Die grobe Einrichtung ist nun abgeschlossen.

Regeln und Zonen einrichten
In den „Firewall-Einstellungen" findest du das Herzstück der Firewall. Hier kannst du Regeln für Anwendungen erstellen oder bearbeiten, globale Regeln einrichten, die höhere Priorität als die Anwendungsregeln haben oder vordefinierte Richtlinien erstellen, um nicht immer dieselben Regeln neu erstellen zu müssen. Der Rest dürfte auch selbsterklärend sein. Wichtig zu wissen ist, dass bei den Regeln immer von unten nach oben gearbeitet wird, d.h. verbietet man in einer Regel das gesamte Internetprotokoll (IP), so kann man mit einer Regel die sich darüber befindet einzelne Protokolle, Ports etc. wieder freischalten.

Fangen wir nun mit der eigentlichen Arbeit an:

Wir erstellen eine neue Netzwerkzone im entsprechenden Reiter, indem wir den winzigen Pfeil unten anklicken und „Hinzufügen" auswählen. Dies ist nötig, wenn sich die lokale IP, die man vom häuslichen Router zugewiesen bekommt, ändern kann. In meinem Netzwerk hat der Router die IP 192.168.178.1 und alle Clients die an den Router angeschlossen werden bekommen via DHCP

automatisch eine IP von 192.168.178.20-200 zugewiesen. In der Netzwerkzone tragen wir also in meinem Fall die IP-Range „192.168.178.20 - 192.168.178.200“ ein. Als Namen habe ich „Heimnetz Computer“ gewählt.

Da Perfect Privacy nun auch unterschiedliche Remoteports (das sind die Ports vom Server) anbietet, erstellen wir nun eine Portgruppe unter dem Reiter „Port-Gruppen“ mit dem Namen „Perfect Privacy OpenVPN“. Hier tragen wir nun nacheinander folgende Ports ein: 1149, 149, 1150, 150, 1151 und 151.

Nun erstellen wir die globalen Regeln (Richtlinien) die immer gleich bleiben und nicht angepasst werden müssen.

- Blockieren, IP Ein von MAC Beliebig nach MAC Beliebig über Protokoll Beliebig
- Blockieren, IP Aus von [Heimnetz Rechner] nach MAC beliebig über Protokoll Beliebig
- Zulassen, TCP Aus von [Heimnetz Rechner] nach IP 192.168.178.1 falls der Quellport Beliebig und der Zielport Beliebig ist
- Zulassen, UDP Aus von [Heimnetz Rechner] nach MAC Beliebig falls der Quellport Beliebig und der Zielport 53 ist
- Zulassen UDP Aus von [Heimnetz Rechner] nach MAC beliebig falls der Quellport Beliebig und der Zielport [PP OpenVPN] ist

Zu 1: unangefragte IP-Pakete werden normalerweise von deinem Rechner nicht benötigt und können somit direkt blockiert/verworfen werden. Solltest du diese trotzdem benötigen, erstelle diese Regel nicht.

Zu 2: Hiermit wird jeglicher Netzwerkverkehr über das Weltnetzprotokoll in das Netz blockiert.

Zu 3: Wird benötigt, damit du noch über den Netzbetrachter auf deinen Router zugreifen kannst. Bei einer abweichenden Router-IP natürlich abändern...

Zu 4: Hierbei werden die DNS-Anfragen, die standardmäßig über den Port 53 laufen, zugelassen. Die VPN-Hostnamen wie zB de3.gigabit.perfect-privacy.com müssen ja in IP-Adressen aufgelöst werden, sofern diese nicht durch die IPs in den Config-Dateien ersetzt wurden.

Zu 5: Hiermit wird der UDP-Traffic zum VPN-Server über die verschiedenen in der Port-Gruppe definierten Ports zugelassen.

Wir bestätigen die Regeln mit OK.

Test
Die Firewall ist nun komplett eingerichtet. Anwendungen wie Firefox oder Windowsdienste müssen natürlich noch im Pop-Up-Fenster zugelassen werden. Diese kann man dann im Pop-Up auswählen und die Firewall sich diese merken lassen.

Was jetzt noch fehlt ist der Test, ob alles funktioniert. Hierfür verbinden wir uns mit einem VPN-Server von Perfect Privacy. Sollte das geklappt haben, disconnecten wir uns vom Server und versuchen im Firefox eine Weltnetzseite aufzurufen. Sollte das nicht funktionieren, so ist unsere Firewall erfolgreich eingerichtet.

8.35 Netzbetrachter („Browser“)

Netzbetrachter, oder allgemein auch Browser sind spezielle Computerprogramme zur Darstellung von Webseiten im Weltnetz oder allgemein von Dokumenten und Daten. Das Durchstöbern des World Wide Webs beziehungsweise das aufeinanderfolgende Abrufen beliebiger Verweise (Hyperlinks) als Verbindung zwischen Webseiten mit Hilfe solch eines Programms wird auch als Internetsurfen bezeichnet.

Neben HTML-Seiten können Webbrowser verschiedene andere Arten von Dokumenten anzeigen.

-5 Gründe auf den Internet Explorer zu verzichten

Der Internet Explorer ist unsicher

Es gibt Unmengen von Sicherheitslücken, durch die sich meistens lokale Daten einsehen und bearbeiten lassen. Wer das nicht glaubt, sollte sich unbedingt die Liste der gefundenen Lücken anschauen.

Falsche Seitendarstellung
Der Internet Explorer zeigt moderne Seiten nicht immer korrekt an. Andere Netzbetrachter halten sich besser an die Standards und bieten somit dem Webdesigner mehr Freiheit, seine Seiten zu gestalten.

Beispiel 1:

Sämtliche bekannte Netzbetrachter können stufenlose PNG-Transparenz ausser der Internet Explorer.
Beispiel 2:

So sollte es aussehen (screenshot mit dem Firefox gemacht - Bilder sind auf der Netzseite zu finden)

So schaut es im Albtraum aus, mh, ich meine im Internet Explorer:

Auch die CSS-Unterstützung beim Internet Explorer ist schlecht implementiert. Es wäre zu viel alles aufzulisten, aber unter www.positioniseverything.net/explorer.html findest du eine gute Zusammenfassung der schlimmsten Fehler.

Kein Open Source

Internet Explorer ist nicht Open Source, das heißt, dass sein Quellcode nicht frei verfügbar ist. Bei Open Source-Netzbetrachtern kann jeder den Quellcode anschauen, der Vorteil ist klar:
Wenn mehr Leute den Quellcode anschauen, werden auch mehr Fehler gefunden, der Netzbetrachter ist sicherer.

Außerdem kann jeder seine Erweiterungen dazugeben, wodurch der Netzbetrachter immer besser wird.

Nicht Plattformunabhängig
Der Internet Explorer ist Plattformabhängig. Microsoft liefert den Internet Explorer nur für Windows und Mac aus, die Mac-Version wird aber (zum Glück) nicht mehr weiterenwickelt. Neuere Internet Explorer sollen sogar eine aktuelle Windows-Version verlangen und zwar nicht, weil sie auf den älteren Betriebssystemversionen nicht mehr laufen würden, sondern weil Microsoft den Benutzer dazu zwingen will, sich eine neue Windows-Version zu kaufen. Alternative Netzbetrachter laufen auf verschiedenen Plattformen wie Linux, Mac, BeOS und benötigen nicht die aktuellste

Version des jeweiligen Betriebssystems.

Wenig Funktionen
Mit dem Internet Explorer entgehen dir eine Menge sehr nützlicher Funktionen, die du von Firefox kostenlos haben kannst.

Der Internet Explorer besitzt kein Surfen mit Tabs, keine Intelligente Suche, keine Live-Lesezeichen, keine intuitive und anpassbare Bedienung, keine so guten Erweiterungsmöglichkeiten, um nur mal die wichtigsten aufzuzählen.

8.36 Mozillas Firefox

Da der Internet Explorer von Microsoft weiterhin der meist attackierte Netzbetrachter (Browser) ist, empfehlen wir die Nutzung von Mozillas Firefox. Dieser bietet neben einer sehr einfachen Bedienung außerdem eine ebenso einfache Verwaltung der Sicherheitsaspekte (Chronik/Verlauf, Cache, Cookies d.h. die Spuren, die man im Netz hinterlässt).

Hier gezeigte Programmversion: 21.0

Nachdem du die Installationsdatei heruntergeladen hast, öffnest du sie mit einem Doppelklick.

Im Installations-Assistenten klickst du nun auf Weiter und kommst dann zur Installationsart. Hier kannst du Standart ausgewählt lassen und wieder mit Weiter bestätigen.

Nun machst du einen Haken bei „Firefox als Standart Browser einrichten". Der Installationsprozess beginnt dann mit Drücken von Installieren.

Ist dies geschehen bestätigst du mit Fertig stellen und das Programm startet.

8.37 Wichtige Einstellungen für deinen Firefox

Beachte diese wichtigen Einstellungen für deinen Firefox. Ohne diese bist du wesentlich unsicherer im Weltnetz unterwegs und unter Umständen Identifizierbar.

- Speichere keine Spuren auf deinem Computer
- Deaktiviere die Datenweitergabe
- Aktiviere TSL 1.2
- Integriere eine Alternative Suchmaschine in den Netzbetrachter
- Alternativen DNS Server einstellen
- WebRTC ausschalten

Speichere keine Spuren auf deinem Computer

Jedesmal wenn du ins Weltnetz gehst, wird alles was du dort siehst auf deinem Computer zwischengespeichert. Bilder die du dir im Weltnetz ansiehst, hast du also auch gleichzeitig auf der Festplatte. Genau so sieht es auch mit Streams aus. Sieht man sich Streams (Video) im Weltnetz an, werden auch diese zwischengesepeichert. Dazu kommt noch der Verlauf und die Chronik. Anhand dieser kann man dein Surfverhalten feststellen und einsehen, auf welchen Seiten du dich

aufgehalten hast ect. (sofern jemand Zugriff auf das System hat).

Nach dem ersten Start von Firefox gehst du im Menü auf Extras ¿ Einstellungen ¿ Datenschutz. Dort machst du einen Haken bei Websites mitteilen, dass ich nicht verfolgt werden möchte. Bei dem Punkt Adressleiste, der nichts anderes ist als die Chronik der Besuchten Weltnetzseiten, hast du 3 Einstellungsmöglichkeiten. Wir empfehlen dir Niemals eine Chronik anzulegen.

Nun springst du weiter zu dem Reiter Sicherheit. Hier machst du, falls vorhanden, die Haken aus den Kästchen Passwörter speichern und Master Passwort verwenden raus. Mit OK kannst du das Fenster jetzt schließen.

Willst du nicht auf den Komfort einer Chronik verzichten empfehlen wir dir auf eine Portable Version des Firefox umzusteigen.

Deaktiviere die Datenweitergabe

Bevor du das Weltnetz genießen kannst, muss nur noch die ab Firefox 21 neu dazugekommene Datenweitergabe, deaktiviert werden.

Es gibt zwei Möglichkeiten in den Firefox-Statusbericht zu gelangen. Der kurze Weg ist oben in der Adresszeile „about:healthreport“ einzutippen. Der zweite Weg besteht darin sich durch das Menü zu wühlen: Hilfe ¿ Firefox-Statusbericht.

Auf der Startseite siehst du ein paar interessante Information. Wie lange braucht dein Firefox bis er gestartet ist, wie viele Add-ons sind installiert, wie viele Minuten hast du den Browser schon genutzt. Doch oben Rechts steht „Datenweitergabe“ auf „An“. Ein einfacher Klick darauf genügt um es zu deaktivieren.

Wenn es eine neue Version von Firefox gibt, aktualisiert sich dieser automatisch selbst und muss lediglich neu gestartet werden.

Aktiviere TSL 1.2

Mozilla Firefox und TSL 1.2. Dir sagt das nichts? Darüber solltest du aber bescheid Wissen, gerade jetzt, wo jeder über die NSA schockiert ist. TSL steht für Transport Layer Security. Unter den etwas ältern Weltnetz-Benutzern dürfte es auch noch als SSL bekannt sein. TLS ist ein hybrid Verschlüsselungsprotokoll und wurde zur sicheren Datenübertragung im Weltnetz erfunden.

Doch wo ist nun das Problem?

In der Zwischenzeit sind wir schon bei der TSL Version 1.2 angelangt. Firefox benutzt aber Stur die ältere Version. Selbst in Version 24, was momentan die aktuellste ist. Zum Vergleich: TSL 1.2 gibt es seit fast schon 5 Jahren.

Wie dem auch sei, wer es jetzt kaum erwarten kann auf TSL 1.2 umzusteigen der navigiert eben ganz schnell zu „about:config“. nachdem du Akzeptiert hast das du auch nichts zerstören wirst suchst du eben schnell nach „TSL“.

Du solltest nun in der Spalte „Einstellungsname“ den Begriff „security.tls.version.max“ finden.

Den Wert in dieser Spalte änderst du nun mit einem Doppelklick in „3“ ab und du surfst nun ein Stück sicherer mit TSL 1.2.

Integriere eine Alternative Suchmaschine in den Netzbetrachter

Mehr Datenschutz bedeutet nicht immer weniger Komfort. Ixquick kann mit sehr wenig Aufwand als Standardsuche in deinen Netzbetrachter integriert werden.

Bei Bedarf danach lässt sich jederzeit auch wieder mit einem Klick auf die vorherige Suchmaschine wechseln und umgekehrt, so dass bisherige Sucheinstellungen nicht ersetzt, sondern um weitere Auswahlmöglichkeiten ergänzt werden.

Das entsprechende Plugin findest du unter **https://www.ixquick.de/deu/download-ixquick-plugin.html**.

Wähle die dabei angebotene Konfiguration „HTTPS“, um die Übertragung der Suchanfragen und Suchergebnisse von und zur Ixquick Suchmaschine zu verschlüsseln und ein sonst an verschiedenen Stellen sehr einfaches Abhören und Protokollieren deiner Suchanfragen zu erschweren.

Wer nicht nur aus guten Gründen Google misstraut, sondern auch den Betreibern und den Datenschutzversprechen von Ixquick nicht gänzlich vertrauen mag, kann Ixquick im Gegensatz zu Google problemlos auch **völlig anonym über den Anonymisierungsdienst Tor** nutzen.

Für alle alternativen Suchmaschinen gilt, dass sie eine andere Sicht auf das Weltnetz bieten und die Ergebnisse sich von Google unterscheiden. Man sollte bei der Beurteilung der Ergebnisse beachten, dass auch Google nicht die reine Wahrheit bieten kann, sondern nur eine bestimmte Sicht auf das Weltnetz.

Alternativen DNS Server einstellen

Wer im Weltnetz surft, gibt entweder den Namen der Weltnetzseite direkt in die Adresszeile ein oder benutzt eine Suchmaschine, um die gewünschte Weltnetzseite aufzurufen.

In beiden Fällen wird die Weltnetztseite jedoch über die sogenannte IP-Adresse aufgerufen, die aus einer gegliederten Nummernfolge besteht, beispielsweise aus 68.146.90.237. Merken kann man sich die nummerische IP-Adresse aber nicht besonders gut. Aus diesem Grund gibt es ein Internetnamensystem und spezielle Server, die diese Namen mit Hilfe des Domain Name System (DNS) wieder in nummerische Adressen auflösen. Die größte und schnellste Ansammlung von DNS-Servern hat wohl Google. Du hast die Möglichkeit, diese gratis zu nutzen, beispielsweise wenn du deinen Provider im Verdacht hast, dass seine DNS-Server ein wenig lahm sind oder mit manchen Weltnetzadressen keine Verbindung aufbauen.

Mittels einer Änderung in der Konfiguration des Netzwerkadapters deines Rechners geben Sie die Anweisung, die DNS-Server von z.B. OpenDNS zu nutzen.

Hierfür klickst du bei Windows Vista und Windows 7 in das Suchfeld des Startmenüs oder bei Windows XP auf „Ausführen“. Nun gibst du ncpa.cpl ein und bestätigst mit der Enter-Taste. Klicke dann mit der rechten Maustaste die aktive „LAN-Verbindung“ oder die „Drahtlosnetzwerkverbindung“ an und im Menü auf „Eigenschaften“. Im Dialogfenster klickst du in der Liste der Verbindungselemente doppelt auf „Internetprotokoll Version 4 (TCP/IPv4)“ oder „Internetprotokoll (TCP/IP)“ (bei Windows XP).

Markiere im folgenden Dialogfenster mit einem Mausklick die Option „Folgende DNS-Serveradressen verwenden“. Sollten in den Feldern darunter bereits Einträge vorliegen, so kann es durchaus sein, dass diese Vorgaben für den Zugriff auf das interne Hausnetzwerk notwendig sind. In diesem Fall solltest du Änderungen nur nach Rücksprache mit dem Systemadministrator deines Netzwerks vornehmen, auf jeden Fall aber die eingetragenen Adressen notieren, um sie gegebenenfalls auf die

hier beschriebene Weise wieder einzugeben.

Wenn lediglich in einem der beiden Felder ein Eintrag vorliegt, gibst du nur im freien Feld eine der beiden folgenden Zahlenfolgen ein.

Klicke nun in das Feld „Bevorzugter DNS-Server“ und gebe hier in die vier durch Punkte getrennten Bereiche die Ziffernfolge 208.67.222.222 ein, wobei du die Einfügemarke mit den Pfeiltasten bewegst. Ebenso gibst danach im Feld „Alternativer DNS-Server“ die Ziffernfolge 208.67.220.220 ein. Bestätige die Eingabe mit einem Klick auf „OK“ und schließe auch das nächste Dialogfenster mit „OK“. Daraufhin erfolgt der Zugang ins Weltnetz über die DNS-Server von OpenDNS. Um die Einstellung wieder zurückzusetzen, öffnest du auf die oben beschriebene Weise das Eigenschaften-Dialogfenster und markierst hier entweder „DNS-Serveradresse automatisch beziehen“ oder trägst die notierten DNS-Server-Adressen wieder in die Felder ein.

WebRTC ausschalten

Wo das Problem in der WebRTC Funktion liegt haben wir im im Blog bereichtet: SfN - Infoblog: Firefox und Chrome verraten IP Adressen trotz VPN.

Wieder kannst du diese Funktion ganz einfach in der „about:config“ ausschalten. Oben in der Adresszeile „about:config“ eintippen und nach dem Wert „media.peerconnection“ suchen. Diesen musst du von „enabeld“ auf „false“ setzen.

8.38 Begrifferklärungen (Browsercheck)

Das World Wide Web ist bunt und vielfältig - doch diese Vielfalt hat ihren Preis. Solange das Web im Wesentlichen aus formatiertem Text mit eingebundenen Bildern bestand, war das Risiko beim Betrachten der Seiten vergleichsweise gering. Immer weniger Web-Sites kommen jedoch ohne JavaScript-Menüs, eingebettete Filme, Spiele oder andere so genannten aktiven Inhalte aus.

Durch diese große Bandbreite an Funktionen und die damit einhergehende Komplexität der Browser schleichen sich immer wieder Programmierfehler ein. Diese beeinträchtigen teilweise die Funktionstüchtigkeit im täglichen Gebrauch (z.B. stürzt der Browser beim Aufruf bestimmter Seiten immer wieder ab). Eine Reihe dieser „Bugs“ genannten Fehler gefährden aber auch die Sicherheit des Rechners, auf dem der Browser läuft. Über speziell präparierte Web-Seiten lassen sich dann Dateien auf der Festplatte lesen oder gar manipulieren oder Viren und andere sogenannte Malware einschleusen.

Erweiterte Browser-Funktionen wie JavaScript, Java, ActiveX und Co. erfordern es, dass fremder Code auf dem Rechner der Besucher ausgeführt wird. Zwar gibt es diverse Sicherheitsmechanismen, die verhindern sollen, dass solcher Code auf dem Rechner Schaden anrichtet. Doch immer wieder werden Sicherheitslücken bekannt, die diese Einschränkungen aushebeln. Viele davon beruhen auf Programmierfehlern und lassen sich durch Installation der aktuellen Browser-Patches beseitigen. Aber manche Risiken sind auch prinzipieller Natur und lassen sich nur durch Deaktivieren der zugehörigen Optionen vermeiden.

Die richtige Browser-Konfiguration für alle Surfer gibt es nicht. Wer seinen Rechner nur zum Spielen benutzt und nebenher ein wenig im Internet surfen will, hat niedrigere Ansprüche an dessen Sicherheit als jemand, der darauf wichtige Firmenunterlagen speichert oder Online-Banking betreibt. Und wenn die persönliche Lieblings-Site nur mit Java funktioniert, muss der Surfer eben abwägen, ob er zugunsten der Sicherheit ganz darauf verzichten will, oder ob er das damit verbundenen Risiko in Kauf nehmen will.

Bei der Suche nach Ihrem persönlichen Kompromiss helfen Ihnen die oben aufgeführten Links. Sie erläutern die einzelnen Browser-Funktionen, demonstrieren deren Missbrauchspotenzial, und zeigen, wie man die entsprechenden Funktionen an- oder abschaltet. Das beste Mittel gegen Schädlinge aus dem Browser ist Wissen darüber gepaart mit gesundem Misstrauen gegenüber allem, was aus dem Netz kommt. Wer auf alles klickt, was ihm irgendwo unterkommt, wird sich früher oder später einen Schädling einhandeln egal welchen Browser oder welches Betriebssystem er nutzt.

Siehe:

- ActiveX
- Cookies
- Java
- JavaScript / JScript
- Phishing
- Virsual Basic Script
- XPI-Erweiterungen

8.38.1 ActiveX

Deine aktuelle Einstellung:
Aufruf sicherer ActiveX-Controls funktioniert nur mit IE

Aufruf unsicherer ActiveX-Controls funktioniert nur mit IE

Microsofts ActiveX-Technologie ist im Bereich Netzbetrachter am ehesten mit den Plug-Ins aus der Mozilla-/ Firefox-/ Netscape-Welt zu vergleichen. Das Steuerelement spielt dabei im Internet-Explorer beispielsweise Multimedia-Dateien ab, die der Web-Server bereitstellt. Ist das entsprechende ActiveX-Control bereits auf dem Rechner installiert, wird es von Windows gestartet und mit den Daten gefüttert. Andernfalls kann der Netzbetrachter das Control auch automatisch aus dem Weltnetz laden.

Ein ActiveX-Control kann auf beliebige Ressourcen des Rechners zugreifen und somit auch beliebigen Schaden anrichten. Der Internet Explorer unterscheidet zwischen signierten und unsignierten Controls. Ein signiertes Control wurde vom Hersteller mit einer digitalen Unterschrift versehen. Ist diese intakt, kann der Benutzer sicher sein, dass das Steuerelement vom Inhaber des verwendeten Zertifikats erstellt und nachträglich nicht verändert wurde. Eine Garantie, dass das ActiveX-Control keinen Schaden anrichtet, hat er damit jedoch nicht. In den Default-Einstellungen fragt der Internet Explorer den Anwender bei signierten ActiveX-Controls, ob er sie herunterladen und installieren darf; unsignierte Controls lädt er nicht.

Des weiteren gibt es die Möglichkeit, via JScript oder VBS (meist lokal installierte) ActiveX-Controls zu aktivieren und zu steuern (wie es auch der Test oben demonstriert). Die Sicherheitseinstellungen unterscheiden hierbei zwischen Controls „die sicher für Scripting sind“ und solchen ohne diese Klassifizierung. Die Einstufung „Sicher für Scripting“ nimmt der Hersteller vor, wenn er der Überzeugung ist, dass das Control keinen Schaden anrichten kann. Es gibt allerdings bereits mehrere Beispiele, bei denen sich im Nachhinein herausgestellt hat, dass diese Einschätzung falsch war.

Dieses Risiko ist nicht zu unterschätzen. Hat nämlich eine Weltnetzseite ein zusätzliches ActiveX-Control installiert - beispielsweise um einen Virencheck des Computers durchzuführen - können

später auch andere, potenziell bösartige Weltnetzseiten dieses Control aufrufen und fernsteuern.

ActiveX-Controls dienen häufig dazu, den Funktionsumfang des Internet Explorer zu erweitern. Realaudio- oder Quicktime-Player können so ihre Multimedia-Dateien direkt im IE-Fenster abspielen. Außerdem bieten Firmen Serviceleistungen wie Online-Virenscans über ActiveX-Controls an. Die Missbrauchsmöglickeiten sind jedoch gewaltig. Benutzer, die Wert auf Sicherheit legen, sollten deshalb alle Optionen mit ActiveX deaktivieren oder zumindest auf „Eingabeaufforderung“ stellen.

Der Internet Explorer kann ebenfalls als ActiveX-Control zum Einsatz kommen. So nutzt beispielsweise Outlook Express das IE-Control zur Anzeige von HTML-eBriefen. Hierfür kommen ebenfalls die Einstellungen der in Outlook Express ausgewählten Sicherheitszone des IE zur Anwendung.

8.38.2 Cookies

Deine aktuelle Einstellung:
Cookies sind AKTIV !

Cookies sind kleine Datenschnipsel, die der Browser auf Anforderung durch einen Web-Server auf der Festplatte ablegt. Sie enthalten - mehr oder weniger kodiert - Informationen, mit denen der Web-Server den Besucher beim nächsten Besuch oder auf den Folgeseiten wiedererkennen kann, meist eine Art Identifikationscode (ID). Die Informationen, die der Server über den Besucher gesammelt hat, speichert er nicht in Cookies, sondern zusammen mit der ID in einer Datenbank. Mit der nächsten Anfrage an den Server liefert der Browser das Cookie automatisch mit, so dass dieser den Benutzer „wiedererkennen“ kann. So sind beispielsweise viele Online-Shops realisiert, bei denen der Besucher über mehrere Seiten hinweg seinen virtuellen Einkaufskorb füllt. Auch viele der personalisierten Seiten auf Portalen arbeiten mit Cookies.

Natürlich können Firmen über Cookies auch Profile über die Vorlieben ihrer Benutzer anlegen. Werbeagenturen wie DoubleClick verteilen mit ihren Anzeigenbannern Cookies auf Tausenden von Web-Sites. So können sie die Surfgewohnheiten im großen Stil verfolgen. Cookies betreffen somit primär die Privatsphäre der Surfer.

Zum Sicherheitsproblem werden Cookies, wenn sie in die falschen Hände gelangen. Normalerweise bekommt ein Server nur die Cookies für seine Domain - also beispielsweise **s-f-n.org** - zu Gesicht. Kann ein Angreifer durch so genannte Cross-Site-Scripting-Angriffe auf fremde Cookies zugreifen, kann er damit unter Umständen die Identität seines Opfers übernehmen und beispielsweise dessen hinterlegte Daten einsehen.

Da inzwischen viele Web-Surfer Cookies abgeschaltet haben, mussten sich die werbetreibenden Datensammler etwas Neues einfallen lassen, das man nicht einfach abschalten kann oder wird. Wie diverse Web-Counter (z.B. der von IVW) bauen sie zum Beispiel vermehrt kleine, 1x1 Pixel große transparente GIF-Dateien in die Seiten ein, so genannte „Web Bugs“.

Man kann zwar den Browser so einstellen, dass er Cookies nur auf Nachfrage akzeptiert. In der Praxis überfluten den Surfer dann jedoch manche Sites mit so vielen dieser Dialogboxen, dass man mit dem Klicken gar nicht hinterherkommt. Als Kompromiss kann man Cookies nur von Servern akzeptieren, deren Seiten man gerade besucht oder die Cookies gelegentlich ausmisten. Firefox und Opera bieten bereits Funktionen, die das selektive Löschen von Cookies ermöglichen. Der Internet Explorer wird eine solche Option in Version 7 enthalten. Wer besonders auf seine Privatsphäre achtet, schaltet die Annahme von Cookies generell ab.

8.38.3 Java

Deine aktuelle Einstellung:
Java ist deaktiviert!

Java wurde von der Firma Sun als plattformübergreifende Programmiersprache entwickelt. Beim ihrem Einsatz auf Weltnetzseiten lädt der Besucher ein kleines Java-Applet, das auf seinem Rechner abläuft. Häufig nutzen Web-Designer solche Applets für zusätzliche Dienste wie Laufbänder mit Newsticker-Meldungen oder drehbare 3D-Darstellungen. Aber auch komplexere Anwendungen, beispielsweise mit Datenbankabfragen, lassen sich in Java realisieren.

Die Java-Programme laufen dabei in einer so genannten Sandbox ab. Das bedeutet, die Applets laufen in einer in sich geschlossenen Umgebung, der Java Virtual Machine (JVM), die keinen Zugriff auf lokale Ressourcen wie Dateien oder Programme hat. Durch dieses Konzept ist Java eigentlich eine sichere Technologie - leider schleichen sich auch bei der Implementierung der JVM gelegentlich Fehler ein, die zu Sicherheitslücken führen. Dann können spezielle Java-Applets beispielsweise doch auf lokale Dateien zugreifen. In der Vergangenheit sind mehrere solcher Sicherheitslücken bekannt geworden.

Java kann in allen Netzbetrachtern separat aktiviert beziehungsweise deaktiviert werden. Wegen einer aktuellen Sicherheitslücke solltest du Java derzeit nicht einsetzen.

Falls Java oben als „aktiv“ angezeigt wird, deaktiviere die Erweiterung im Netzbetrachter oder deinstalliere Java komplett:

Java-Plug-in unter Firefox deaktivieren
Plug-ins unter Chrome deaktivieren
Java-Plug-in unter Safari deaktivieren

Unter Opera erreicht man die Plugin-Verwaltung durch die Eingabe von:
opera:plugins

in die Adressleiste. Beim Internet Explorer genügt das Deaktiveren der Plug-ins unter „Add-Ons verwalten“ nicht. Wer den IE einsetzt, sollte Java daher besser vollständig über Systemsteuerung/Software deinstallieren.

8.38.4 JavaScript / JScript

Deine aktuelle Einstellung:
JavaScript ist AKTIV !

Erstmal vorweg:
Java und Javascript sind nicht dasselbe!

Beides sind Programmiersprachen doch während JavaScript fest in jedem Browser verankert ist und jede Webseite JavaScript-Anweisungen enthalten kann, muss zum Ausführen von Java-Programmen eine Erweiterung installiert sein. Sicherheitsprobleme gibt es in beiden Welten.

Fast wöchentlich werden neue Lücken in Java bekannt, und das trotz der Bemühungen von Hersteller Oracle, diese zeitnah zu stopfen. Viele Computer-Benutzer fragen sich daher, ob es nicht besser ist, wegen dieser Probleme nicht nur auf Java, sondern auch gleich auf JavaScript zu verzichten - das ist aber nicht unbedingt ein Vorteil.

Während Java eine höhere Programmiersprache ist, mit der man Software erstellen kann, wird JavaScript heute meist in Webseiten für die Interaktion verwendet, etwa um einer Seite Leben einzuhauchen. Es gibt zwar auch hier Sicherheitsrisiken, allerdings vergleichsweise wenige. Java-Apps hingegen haben Zugriff auf den Computer und können deswegen größere Sicherheitsprobleme verursachen.

Für JavaScript gibt es eine Reihe von Anwendungsmöglichkeiten, die von Spielereien bis zu sinnvollen Ergänzung einer Weltnetzseite reichen.

Typische Anwendungsgebiete von JavaScript sind:

- Dynamische Manipulation von Webseiten über das Document Object Model
- Plausibilitätsprüfung (Datenvalidierung) von Formulareingaben noch vor der Übertragung zum Server
- Anzeige von Dialogfenstern, Lightboxes
- Senden und Empfangen von Daten, ohne dass der Browser die Seite neu laden muss (Ajax)
- Sofortiges Vorschlagen von Suchbegriffen (suggesting search)
- Banner oder Laufschriften
- Verschleierung von E-Mail-Adressen zur Bekämpfung von Spam.
- Mehrere Frames auf einmal wechseln oder die Seite aus dem Frameset „befreien“

Die am häufigsten anzutreffende Anwendung sind Menüs und der Austausch von Bildern beim Überfahren mit der Maus („Mouse-Over-Effekt“, „Hover-Buttons“). Beispiel Mouse-Over-Effekt: Smile :-) MouseOver
Einige Anwendungen, die mit JavaScript möglich sind, werden als „schlechter Stil“ angesehen. Viele davon können deshalb inzwischen auch vom Browser blockiert werden.
Beispiele:

- Quelltext „verschleiern“, um diesen vor dem Besucher zu verstecken
- Verschleiern von Internetadressen, auf die ein Link verweist
- Deaktivieren des Kontextmenüs, um zu erschweren, dass Bilder oder die gesamte Seite abgespeichert werden können
- Deaktivieren der Kopierfunktion, um zu erschweren, dass Texte oder Bilder kopiert werden können
- Unaufgeforderte (Werbe-)Pop-ups oder Pop-unders
- Ungewolltes Öffnen von Fenstern, teilweise auch Öffnen beliebig vieler Fenster
- Ungewolltes Schließen des Browserfensters
- Ungewollte Größenänderung des Browserfensters
- Blockieren der Anwender mit zahllosen aufeinanderfolgenden Dialogfenstern
- Bei anfälligen Webanwendungen kann JavaScript auch von Dritten missbraucht werden, etwa per XSS (Codeeinschleusung).
- JavaScript-Navigation.

- Barrierearme Webseiten zeichnen sich dadurch aus, dass sie auch bei abgeschaltetem JavaScript möglichst uneingeschränkt navigierbar bleiben. Oft schränkt das nicht aktivierte JavaScript die Benutzbarkeit einer Webseite ein.

Aktuelle Netzbetrachter führen JavaScript nur in einer Sandbox aus. In diesem „Sandkasten“ können sie nur wenig Unheil anrichten, da kein direkter Zugriff auf Hardware oder Festplatte möglich ist aber wenn sich z.B: beim Besuch einer Seite automatisch weitere Browser-Fenster öffnen, ist meist JavaScript im Spiel. Es ist prinzipiell sehr einfach, den Rechner durch Hunderte von zusätzlichen Fenstern lahmzulegen. (Dieser Link öffnet nur eines.) Die meisten der bekannt gewordenen Sicherheitslücken in Netzbetrachtern sind eng mit JavaScript verknüpft. Wo es nicht Hauptgegenstand des Bugs ist, benötigt man es häufig, um die Sicherheitslücke ausnutzen zu können. Da immer mehr Webseiten mit deaktiviertem JavaScript kaum bedienbar sind, sollte JavaScript nur eingeschränkt eingeschaltet bleiben.

Wie du JavaScript kontrollierst erfährst du im NoScript Leitfaden auf den nächsten Seiten.

8.38.5 Phishing

Phishing ist ein Kunstwort für das „Abfischen“ von Zugangsdaten wie Passwörter und PINs. Typischerweise versenden die Daten-Phisher Massen-eBriefe, die das Aussehen der Nachrichten der Online-Bank oder eines Shops raffiniert imitiert. Einige sehen aus wie schicke Formbriefe mit Kopf und Firmenlogo und stammen scheinbar von einem glaubwürdigen Absender.

Typische Phishing-eBriefe behaupten, es habe eine Software-Umstellung gegeben und deshalb soll der Benutzer unbedingt eine in der Nachricht angegebene Weltnetzadresse ansteuern und dort seine Kreditkartennummer erneut eingeben. Oder es gäbe Hinweise auf einen Missbrauch des Accounts, weshalb der Kunde eine im Brief angegebene Adresse ansteuern und dort sein Passwort und andere Account-Infos eingeben müsse.

Immer geht es darum, den Benutzer auf eine Weltnetzseite zu locken, die der des Shops oder der Bank ähnelt. Durch die verschiedensten Tricksereien schaffen es die Betrüger häufig auch, dass die URLs der von ihnen aufgesetzten Seiten denen, der sie vorgeben zu sein, stark ähneln.

Der beste Schutz vor Phishing ist daher große Vorsicht bei einschlägigen eBriefen; Online-Shops und -Banken sollte man nicht durch den Klick auf Links in eBriefen aufsuchen, sondern immer selbst in das Adressfeld des Netzbetrachters eingeben. Auch die Netzbetrachter versuchen den Benutzer zu schützen, indem sie ihn bei verdächtigen Weltnetzseiten warnen. Weitere Informationenn zum Thema Phishing findest du im SfN Informationsblog.

8.38.6 Virsual Basic Script

Deine aktuelle Einstellung:
VBS ist nur mit IE verfügbar!

Visual Basic Script (VBS) ist eine von Microsoft für Client-seitiges Scripting vorgesehene Sprache und stellt eine Untermenge der Funktionen von Visual Basic for Applications (VBA) bereit, der Makrosprache von Microsoft Office. VBS funktioniert nur mit dem Internet Explorer ab Version 4.0, andere Netzbetrachter unterstützen VBS nicht. Im Weltnetz wird es für Client-seitiges Scripting kaum verwendet, meist erhält hier JavaScript/JScript den Vorzug.

Dafür erfreut es sich jedoch großer Beliebtheit bei Autoren von Viren und Würmern. Diese betten VBS-Code in HTML-eBriefe ein. Bei zu laschen Sicherheitseinstellungen führen eBrief-Programme, die den Internet Explorer zur Darstellung von HTML-eBriefen nutzen, den VBS-Code aus. VBS-Schadcode kann auch über angehängte HTML-Dateien zur Ausführung gelangen. VBS lässt sich

im Internet Explorer nur gemeinsam mit JScript unter der Option „Active Scripting“ ein- oder ausschalten.

8.38.7 XPI-Erweiterungen

Firefox, Mozilla und die darauf aufbauenden Netscape 7.x-Versionen lassen sich über „Cross Platform Installable files“ - kurz XPIs - um zusätzliche Funktionen erweitern. Diese Browser-Erweiterungen kann man im Menü Extras/Erweiterungen verwalten. Auch das eBrief-Programm Thunderbird kann solche XPI-Plug-Ins einbinden.

XPI-Erweiterungen sind beliebt. Auf der Übersichtsseite von Mozilla.org finden sich mehr als 1000 Add-Ons aller Art. Zu ihrer Popularität hat auch beigetragen, dass sich die XPIs bequem mit wenigen Mausklicks installieren lassen. Allerdings sollte man sich dabei der Tatsache bewusst sein, dass die Installation Programme ausführt, die prinzipiell auch Spyware und Dialer einschleppen können. In der Vergangenheit haben die Mozilla-Abkömmlinge diese Installation etwas lax gehandhabt, so dass ein voreiliger Mausklick genügte, um sich Unrat einzufangen.

Als zusätzlichen Schutz hat Mozilla beim Installationsvorgang eine zweistufige Warnung eingebaut. Zunächst muss der Benutzer die Herkunfts-Website des XPI in die Liste der Sites aufnehmen, die bei ihm Erweiterungen installieren dürfen. Vor der endgültigen Installation schaltet Firefox dann noch eine fünfsekündige Denkpause mit einer Sicherheitswarnung. Der beste Schutz besteht allerdings darin, Add-Ons nur von vertrauenswürdigen Sites zu installieren, etwa von der Download-Seite bei Mozilla.org.

Um dem Benutzer verlässliche Informationen über die Herkunft eines XPIs zu geben, gibt es theoretisch die Möglichkeit, diese digital zu signieren. Mangels Infrastruktur gibt es allerdings in der Praxis so gut wie keine signierten Erweiterungen. Auf den nächsten Seiten stellen wir dir einige Add-Ons vor die wir aus sicherheitsgründen Empfehlen.

8.39 Mehr Sicherheit durch Add-Ons

Was ist ein Add-On?

Add-Ons sind kleine Software-Pakete, die neue Funktionen zu deiner Installation von Firefox hinzufügen. Add-ons können Firefox um neue Fähigkeiten erweitern, Wörterbücher anderer Sprachen installieren, oder das Aussehen der Anwendung verändern. Durch Add-Ons kannst du Firefox so personalisieren, dass es deinen Anforderungen und deinem Geschmack genau entspricht.

Wir empfehlen dir folgende Add-Ons damit du dich ein wenig sicherer, mit deinem Firefox, im Weltnetz bewegen kannst:

- Flash und Java blockieren mit FlashBlock und QuickJava
- JavaScript blockieren mit NoScript
- HTTP Referrer beliebig verändern
- HTTPS Finder
- Adblock Plus - Für ein Web ohne nervige Werbung
- Long URL Please
- Bloody Vikings

- User Agent Switcher
- Tracking (Verfolgung durch Webseiten) verhindern

Add-Ons auf aktualität prüfen

Hier zeigen wir dir wie du im Firefox, Add-Ons auf ihre aktualität prüfen kannst. Das geht mit wenigen Klicks, bringt aber sehr viel Sicherheit. Wenn du diese Weltnetzseite studiert hast, weißt du, das über veraltete Add-On/Plugin Versionen Cracker (umgangsprachlich: Hacker) in dein System gelangen können.

Als erstes öffnst du den Firefox Netzbetrachter, gehst auf Extras und klickst dann auf Add-ons.

Dort klickst du auf das Zahnrad und überprüfst die Aktualität der installierten Add-Ons. Gleichzeitig kannst du „Add-Ons automatisch Aktualisieren“ anhaken.

Sollte ein Add-On eine bekannte Schwachstelle haben, wirst du extra darauf hingewiesen. Aber auch alle anderen Add-Ons solltest du aktuell halten, auch wenn es Zeit kostet. Die Zeit und Nerven die du damit einsparen kannst, solltest du mal Malware auf dem Computer haben, rentiert sich.

Es empfiehlt sich diesen Test alle paar Wochen ein mal durchzuführen. Je öfters desto besser.

-Flash und Java blockieren mit FlashBlock und QuickJava

Flash ist neben Java eine *der* Sicherheitslücken. Mit FlashBlock für Firefox sorgst du dafür, dass Flash nur dort läuft, wo du das ausdrücklich erlaubst. Mit QuickJava für Firefox schaltest du außerdem schnell Flash und Java ein und aus.

Adobe Flash ist eine Technik, die Weltnetzseiten interaktiver macht. Dazu bildet Flash eine Art Mini-Computer ab, in dem sich multimediale und interaktive Inhalte darstellen lassen, Grafiken und Video sind damit ebenso möglich wie die Aufzeichnung von Inhalten beim User per Tastatur, Mikrofon und Kamera.

Ein sehr mächtiges Werkzeug also, das auf fast jedem Netzbetrachter installiert ist. Und wie das so ist: Flash hat sehr häufig Sicherheitslücken, und weil Flash mächtig und verbreitet ist, sind damit auch die Sicherheitlücken mächtig verbreitet.

Das alles wäre halb so schlimm, wäre da nicht zusätzlich folgender fataler Umstand wirksam: Sobald du eine Weltnetzseite aufrufst, die ein Flash-Element enthält, wird dieses automatisch gestartet. Sprich: Die Sicherheitlücke von Flash ist ununterbrochen automatisch aktiviert und nicht mit Bordmittel abschaltbar (außer, man deinstalliert es).

Zusammengenommen ergibt sich die reale Gefahr sogenannter „drive-by infections“, das heißt, ein PC wird „im Vorbeisurfen“ infiziert, weil 1. der Nutzer eine Webseite anschaut, 2. die Flash-Malware darauf automatisch startet und 3. den Rechner des Nutzers infiziert, ehe dieser reagieren kann. Manuelle Downloads sind nicht nötig, denn Flash-Inhalte lädt jeder übliche Browser ganz von selbst automatisch herunter. Flash blockieren mit FlashBlock

Hier gezeigte Programmversion: 1.5.17

Als erstes öffnst du den Firefox Netzbetrachter, gehst auf Extras und klickst dann auf Add-ons.

Es hat sich nun der Add-ons-Manager geöffnet und du gibst in das Suchfeld FlashBlock ein und bestätigst mit Enter.

An der ersten Stelle ist auch schon das gesuchte Add-on. Nach einem Klick auf Installieren läd Firefox das kleine Helferlein herunter und installiert es.

Nach der Installation muss der Firefox Netzbetrachter neu gestartet werden damit das Add-on aktiv wird.

Die Browser-Erweiterung macht nichts anderes, als alle Flash-Objekte zu blockieren - alle mit Ausnahme der Flash-Objekte auf Weltnetzseiten, die du selbst in einer Whitelist erlaubt hast. Die Whitelist ist also eine Liste mit Ausnahmen, alle nicht in der Whitelist verzeichneten Seiten befinden sich automatisch in der Blacklist, der Schwarzen Liste der sicherheitshalber „verbotenen" Sites. Das verhindert relativ wirkungsvoll „drive-by infections" auf fremden Websites.

Jede Weltnetzseite mit Flash ist also per Vorgabe geblacklistet: es passiert erst mal nichts, und statt der Animation siehst du einen leeren Bereich dort, wo die Animation zu sehen wäre, mit Play- oder Flash-Symbol.

Du hast dann zwei Möglichkeiten:

1. Du klickst auf den Abspielen-Button, und FlashBlock erlaubt einmalig die Wiedergabe dieser Flashanimation. Diese Erlaubnis gilt nur für dieses eine Mal und auch nur für dieses eine, durch den Play-Button sichtbare Flash-Element. Dabei muss klar sein: Wenn du „irgendwo im Web", „irgendeiner Weltnetzseite" diese Erlaubnis erteilst, auch wenn sie nur einmalig gilt, kann dich das infizieren. Nutze das also wirklich nur auf Seiten, die du für vertrauenswürdig hälst.
2. Alternativ klickst du mit der rechten Maustaste auf den leeren Bereich des Flash-Elements und wählst Flash für diese Website erlauben. FlashBlock erlaubt dadurch dauerhaft die Wiedergabe von Flash-Animationsgerümpel auf allen Seiten der aktuellen Webadresse.

Erlaubst du zum Beispiel youtube.com oder clipfish.de, dann funktioniert Flash in Zukunft auf allen Seiten dieser Portale ohne weitere Nachfrage. Wer also seine wichtigsten Portale nach und nach wie im Screen sichtbar in die Whitelist aufnimmt, büßt letzlich keinen Komfort ein. Und trotzdem wirkt FlashBlock auf unbekannten, neuen Weltnetzseiten. Flash und Java blockeren mit QuickJava

Hier gezeigte Programmversion: 1.8.1.1

Wie du dieses Add-On herunterladen kannst sollte klar sein. Statt „FlashBlock" gibst du in die Add-On Suchmaske nun „Quickjava" ein und installierst es.

QuickJava für Firefox führt keine Whitelist. Statt dessen hast du damit eine Reihe von Buttons rechts unten im Netzbetrachter, mit denen du ganz einfach an- und abschalten kannst, ob JavaScript, Java, Flash, Silverlight und Cookies derzeit generell aktiviert sind oder nicht.

Ein einfaches Anklicken schaltet zwischen aktiviert und deaktiviert um.

Rot = blockiert
Blau = erlaubt

Hier unsere Empfehlung:
JS (JavaScript) erlaubt, J (Java) verboten, F (Flash) verboten, SL (Silverlight) verboten, C (Cookies) erlaubt.

Und wenn du unbedingt mal Flash (oder Java) brauchst, dann schalte es halt ein, indem du auf F (oder J) klickst. Dann sieht es so aus: JS (JavaScript) erlaubt, J (Java) verboten, F (Flash)

erlaubt, SL (Silverlight) verboten, C (Cookies) erlaubt.

Drücke dann F5 um die Seite neu zu laden und siehe da: Flash geht - bzw: *jetzt* entscheidet FlashBlock, ob es geht oder nicht.

Sobald du Flash nicht mehr brauchst, schalte es wieder ab.
Warum zwei Blocker?

Ganz einfach:

Eigentlich würde QuickJava ja reichen: Immer J/F/SL blockieren und nur nutzen, wenn man es wirklich braucht - das schafft mehr Sicherheit. Aber man vergisst einfach, Flash wieder zu sperren, wenn man es gebraucht hat. Das ist einfach so. Dann wirkt immer noch FlashBlock, über das du Flash nur auf bestimmten, einigermaßen vertrauenswürdigen Seiten gestattest.

Sprich: Wenn du an alles denkst, hast du mit FlashBlock + QuickJava stets einen doppelten Blocker aktiv. Wenn du mal wieder vergessen hast - mir jedenfalls passiert es dauernd - Flash in QuickJava wieder abzuschalten, dann wirkt immer noch FlashBlock gegen die Möglichkeit, sich auf den zufälligen und daher eher gefährlichen Seiten aus Suchmaschinen-Suchergebnissen eine „drive-by infection“ zuzuziehen.

8.40 JavaScript blockieren mit NoScript

Im Normallfall wird kein seriöser Webseiten-Betreiber versuchen, mit Javascript groben Unfug anzustellen - schließlich sollst du ja mal wieder bei ihm reinschauen....

Wer aber häufig auf Seiten mit undurchsichtigen Inhalten - insbesondere aus fremdsprachlichem Ausland - unterwegs ist, der sollte Javascript allerdings wohl besser deaktivieren!

Oft wird Malware über Skripte von Drittanbieter in eine Seite eingeschleust; mit NoScript kein Problem, wenn man nur Skripte von der eigentlichen Seite zulässt. Außerdem gibt es noch einen Schutz vor potentiellen Cross-Site-Scripting oder kurz XSS Attacken. Eine genauere Beschreibung was es mit einer XSS Attacke auf sich hat, findest du im Kurzleitfaden Datenschutz.

Hier gezeigte Programmversion: 2.6.4.4

Als erstes öffnst du den Firefox Netzbetrachter, gehst auf Extras und klickst dann auf Add-ons.

Es hat sich nun der Add-ons-Manager geöffnet und du gibst in das Suchfeld NoScript ein und bestätigst mit Enter.

An der ersten Stelle ist auch schon das gesuchte Add-on. Nach einem Klick auf Installieren läd Firefox das kleine Helferlein herunter und installiert es.

Nach der Installation muss der Firefox Netzbetrachter neu gestartet werden damit das Add-on aktiv wird.

Wenn Firefox nun wieder offen ist und du eine Seite besuchst wirst du merken das NoScript aktiv ist. Wie du auf dem Bild siehst wird z.B. auf unserer Seite der Slider u.a. nicht angezeigt, dafür aber ein Hinweistext. Am unteren Bildschirmrand kommt der Hinweis, das momentan Scripte verboten sind, links neben der Adresszeile siehst du das NoScript Symbol.

Wie bei jeder White-List, muss sie erstmal eingerichtet werden. Dazu gehst du jetzt zum Beispiel auf s-f-n.org. Klickst du nun auf das NoScript Symbol kannst du auswählen das alle Beschränkungen aufgehoben werden sollen. Das heißt auf der Seite werden alle Skripte erlaubt, auch die Skript Teile die auf andere Seiten verweisen. Deshalb ist das nicht unbedingt notwendig. Bei uns klickst du zum Beispiel nur auf „s-f-n.org“ erlauben.

Um Skripte zu verbieten, musst du einfach wieder auf das NoScript Symbol klicken, und in der Liste dann „name.TLD verbieten“ anwählen.

Jedesmal wenn nicht alle Skripte auf einer Seite erlaubt sind gibt NoScript eine Meldung aus, diese lässt sich aber ganz ausblenden, oder sie blendet sich nach beliebigen Sekunden automatisch aus. Klicke dazu in dieser Leiste auf Einstellungen und dann abermals auf Einstellungen. Da musst du dann in den Reiter „Benachrichtigungen“, dort kannst du ganz oben bei der Checkbox „Informationsleiste anzeigen, wenn Skripte blockiert werden“ auswählen, ob sie angezeigt werden soll oder nicht. Wenn du willst das sie sich automatisch ausblendet, musst du die 3. CheckBox von oben auswählen, und dort dann deine gewünschte Sekunden Zahl eingeben. Klicke dann auf „Ok“.

NoScript ist im Firefox aufjedenfall ein Skript, das nicht fehlen sollte. Auch wenn es am anfang nervig ist die White-List zu erstellen, so ist es aber im Vergleich zum großen Schutz vor Malware, eine Kleinigkeit.

8.41 HTTP Referrer beliebig verändern

Der HTTP-Referrer verrät von welcher Seite du gekommen bist. Das heißt also, wenn du gerade auf dieser Seite unterwegs bist und dann auf einen Link klickst, sieht der Host-Betreiber der Webseite das du von meiner Webseite gekommen bist, anhand des HTTP-Referrer. Wer also möchte das die Host-Betreiber nicht mehr wissen woher die Besucher bzw. du kommst, kann den HTTP-Referrer abschalten oder verändern.

Hier gezeigte Programmversion: 0.8.16

Als erstes öffnst du den Firefox Netzbetrachter, gehst auf Extras und klickst dann auf Add-ons.

Es hat sich nun der Add-ons-Manager geöffnet und du gibst in das Suchfeld RefControl ein und bestätigst mit Enter.

An der ersten Stelle ist auch schon das gesuchte Add-on. Nach einem Klick auf Installieren läd Firefox das kleine Helferlein herunter und installiert es.

Nach der Installation muss der Firefox Netzbetrachter neu gestartet werden damit das Add-on aktiv wird.

Gehe, wenn der Firefox offen ist, wieder in den Add-On Manager und Navigiere im Menü zu „Erweiterungen“. Dort sollte sich nun „RefControl“ befinden. Klicken dann auf die Einstellungen von RefControl.

Klicke im Einstellungs-Fenster dann unten rechts auf „Bearbeiten“.

Hier hast du die Wahl zwischen:

Normal - aktuellen Referer senden
Blockieren - keinen Referer senden
Ersetzen - Stammadresse dieser Seite senden

Spezifisch

Mit Spezifisch kannst du einen beliebigen Text nehmen (z.B. http://www.de.metapedia.org/bot). Wenn du dich dann entschieden hast klicke auf „OK“ im ersten- und im zweiten Fenster.

Um zu Testen ob auch alles geklappt hat Rufe diesen Link hier auf: www.ip.s-f-n.org

Wenn alles geklappt hat kommt nun der von dir angegebene Link. Wenn nicht, lösche alle Cookies und probiere es nocheinmal. Sollte es dann immer noch nicht geklappt haben, hast du etwas falsch eingestellt.

8.42 HTTPS Everywhere

HTTPS Everywhere ist eine Erweiterung für den Mozilla Firefox Netzbetrachter, mit dem Ziel, die Verbindungen zu Weltnetzseiten automatisch verschlüsselt anzufordern. Es wird als freie Software von der Electronic Frontier Foundation (EFF) in Zusammenarbeit mit dem Tor Project entwickelt.

Vielleicht ein bisschen Aufklärung (in vereinfachter Form), was HTTPS ist:

HTTPS ist eine Erweiterung von HTTP, also dem ganz normalen Protokoll, mit dem du Webseiten abrufst. Das S steht dabei für „Secure“. HTTP überträgt die Daten im Klartext, das ist unsicher. HTTPS benutzt moderne kryptographische Methoden, um die Verbindung zwischen dir und dem Server zu verschlüsseln. Damit kann kein Dritter die Verbindung belauschen, denn er würde nur verschlüsselte Informationen bekommen.

HTTPS wird heutzutage von vielen Seiten verwendet, gerade wenn es um sensible Daten geht. Wenn eine Seite sowohl HTTPS als auch HTTP Verbindungen erlaubt, würde das Tool also, wenn es richtig arbeitet, automatisch die sicherere Version vorziehen. Es ist aber in erster Linie eine Option des Servers. Dieser muss eine solche sichere Verbindung zulassen.

Wenn er dies nicht tut, kann dein Tool auch nichts anderes machen, als das HTTP Protokoll zu verwenden.

Leider gibt es das Add-On nicht wie die anderen im Firefox Add-On Manager. Dies ist aber überhaupt kein Problem, die Eletronic Frontier Foundation (EFF) bietet ihr Add-On HTTPS Everywhere für Mozilla Firefox an zum kostenlosen Download an.

8.43 Adblock Plus - Für ein Web ohne nervige Werbung

Das Firefox Add-On „Adblock“ verwendet eine „Schwarze Liste“ (Black list), welche alles blockt, was darin aufgenommen wird. Das können einzelne Seitenelemente sein, aber auch ganze Server oder sogar komplette Domains. Diese Schwarze Liste ist nach der Installation von Adblock zunächst leer. Du musst nach der Installation von Adblock also zunächst definieren, was geblockt werden soll.

Die Erkennung kann auch über frei wähl- und abonnierbare Liste geschehen, die regelmäßig aktualisiert werden. Eine der bekanntesten Listen ist die so genannte „Easylist“. Zusätzlich zu dieser internationalen Standartliste gibt es die „Easylist Germany“ und die „Easyprivacy“. Letztere blockt Werbeeinblendungen und -skripte.

Hier gezeigte Programmversion: 0.85

Als erstes öffnst du den Firefox Netzbetrachter, gehst auf Extras und klickst dann auf Add-ons.

Es hat sich nun der Add-ons-Manager geöffnet und du gibst in das Suchfeld Adblock Plus ein und bestätigst mit Enter.

An der ersten Stelle ist auch schon das gesuchte Add-on. Nach einem Klick auf Installieren läd Firefox das kleine Helferlein herunter und installiert es.

Nach der Installation muss der Firefox Netzbetrachter neu gestartet werden damit das Add-on aktiv wird.

Adblock einrichten

Klicke nach dem Neustart Firefox auf Extras ¿ Adblock ¿ Preferences und dann auf Adblock Options. Folgende Punkte sollten markiert sein:

Obj-Tabs
Collapse Blocked Elements
Check Parant Links
Site Blocking

Werbung mit der Firefox Erweiterung Adblock filtern

Wenn du auf einer Seite mit Werbung bist, gibt es zwei Möglichkeiten, diese mit dem Firefox-Werbeblocker Adblock zu filtern.

Ein einzelnes Element blocken:

Klicke mit der rechten Maustaste auf das betreffende Werbeelement (z. B. ein Bild oder ein iframe) und bestätige die Meldung Adblock Image im folgenden Fenster mit OK. In Zukunft wird dieses einzelne Element nicht mehr angezeigt.

Meist kommt die Werbung jedoch von einer bestimmten Quelle, so dass es sinnvoller ist, diese Quelle selbst lahmzulegen anstatt einzelne Elemente separat zu blocken. Mehrere Elemente einer bestimmten Quelle blockieren:

Klicke auf Adblock rechts unten in der Statuszeile des Browserfensters oder wähle unter Extras ¿ Adblock List All Blockable Elements aus. Adblock zeigt nun eine Liste von Elementen an, die auf dieser Webseite geblockt werden können. Hier kann man ebenfalls einzelne Elemente auswählen, aber sinnvoller ist es mit dem Platzhalter (Wildcard) * gleich alle Elemente von einer bestimmten Quelle zu filtern, insbesondere da sich der URL eines einzelnen Werbeelements auch ändern kann.

Angenommen du findest folgende Liste:

http://www.irgendeinedomain.de/RealMedia/ads/adstream_lx.ads/1419.....

http://www.irgendeinedomain.de/RealMedia/ads/adstream_lx.ads/7314.....

http://www.irgendeinedomain.de/RealMedia/ads/adstream_lx.ads/4587.....

Klicke nun einen Eintrag in der Liste an und ändere den Eintrag in der Zeile New Filter in www.irgendeinedomain.de/RealMedia/ads/* um. So werden alle Elemente blockiert, die aus dieser Quelle stammen. Wenn du dir an Hand des URLs nicht sicher bist, ob es sich bei einem Element um Werbung handelt, dann kannst du die Seiteninformationen von Firefox zu Hilfe nehmen. Dazu

unter Extras ¿ Seiteninformationen ¿ Medien die einzelnen Elemente anklicken, welche dann zur Identifizierung grafisch angezeigt werden.

An den URLs kann man meist sehr schön sehen, dass diese zu einem Werbeserver gehören.

(Zum Beispiel: http://adserv.quality-channel.de/images/symantec/banner_300.gif)

Hier macht es Sinn, nicht nur diesen einen Server mit adserv.quality-channel.de/* zu blocken (es könnte mehrere Server wie adserv1 oder adserv2 geben), sondern am besten gleich die ganze Domain mit quality-channel.de zu blockieren.

In diesem Fall musst du keinen Platzhalter verwenden, da du die Option Site Blocking (siehe oben) in Adblock aktiviert hast. Es werden alle Elemente von quality-channel.de gefiltert.

Nach der Installation von Adblock empfiehlt es sich, zuerst eine vorgefertigte Liste mit Werbeseiten zu importieren. Eine regelmäßig aktualisierte Filterliste findest du auf www.pierceive.com/filtersetg. Speicher die neueste Version der Liste als Textdatei auf deinem Rechner. Klicke dann auf Extras ¿ Adblock ¿ Preferences und wähle dann unter Adblock Options die Option Import filters ... Suche nun die eben heruntergeladene Adblock List und wähle diese aus. Die Erweiterung Adblock Filterset.G Updater prüft automatisch, ob neue Versionen der Filterliste vorhanden sind. Fälschlicherweise gefilterte Elemente aus der Filterliste entfernen

Um versehentlich gelöschte Werbung wieder sichtbar zu machen gibt es zwei Möglichkeiten:

Komplette Filterliste löschen und neu importieren

Die komplette Filterliste zu entfernen ist die schnellste Möglichkeit, wenn versehentlich blockierte Elemente wieder angezeigt werden sollen.

Klicke dafür auf Extras ¿ Adblock und dann auf Preferences. Wähle nun Adblock Options und schließlich Remove all filters.

Der Nachteil dieser Lösung ist, dass dabei alle selbst erstellten Filter gelöscht werden und du danach erst wieder eine neue Filterliste erstellen oder importieren musst. Ein einzelnes Element aus der Filterliste entfernen

Merke dir zunächst den Dateinamen des betreffenden Elements. Wenn du dir nicht sicher bist, wie das versehentlich geblockte Element heißt, klicke rechts unten in der Statuszeile des Browserfensters auf Adblock. Die kursiv und in roter Farbe geschriebenen Elemente werden von Adblock nicht angezeigt. Schließe das Fenster wieder.

Wähle dann unter Extras ¿ Adblock List den Punkt All Blockable Elements aus. Suche das entsprechende Element und klicke es mit rechts an. Wähle nun Delete.

8.44 Long URL Please

Dank dem „Long URL Please“ Add-On für deinen Firefox siehst du sofort, welche Adresse sich hinter einer Kurz-URL versteckt.

Sogenannte Kurz-URLs sind eine praktische Idee um lange, kryptische Web-Adressen platzsparend zu verschicken oder sich zu merken. Jedoch birgt dieses Verfahren auch erhebliche Sicherheitsrisiken - so ist von außen nicht ersichtlich, wohin der Link führt.

Die Erweiterung „Long URL Please“ für den Firefox nutzt den Dienst „longurlplease.com“, um die Tiny-URLs aufzuschlüsseln. Die Links werden einfach ausgetauscht. Derzeit werden 81 Tiny-URL-Dienste unterstützt.

Hier gezeigte Programmversion: 0.5.1

Als erstes öffnst du den Firefox Netzbetrachter, gehst auf Extras und klickst dann auf Add-ons.

Es hat sich nun der Add-ons-Manager geöffnet und du gibst in das Suchfeld Long URL Please ein und bestätigst mit Enter.

An der ersten Stelle ist auch schon das gesuchte Add-on. Nach einem Klick auf Installieren läd Firefox das kleine Helferlein herunter und installiert es.

Nach der Installation muss der Firefox Netzbetrachter neu gestartet werden damit das Add-on aktiv wird.

Du gehst jetzt noch einmal in den Add-ons-Manager. Dort suchst du dir das Add-On und klickst auf Optionen und stellst es so ein wie auf dem Bild zu sehen ist.

Im nächsten Bild siehst du was genau dieses Add-On bewirkt.

8.45 Bloody Vikings

Das Firefox Add-On vereinfacht die Nutzung von Wegwerf-eBrief-Adressen. Nach der Installation kann ein bevorzugter Dienst für die Wegwerfadressen gewählt werden. Damit kannst du deine eigene eBrief Adresse schützen, indem du auf weniger vertrauenswürdigeren Seiten nicht deine eigentliche eBrief Adresse eingibst.

Hier gezeigte Programmversion: 0.5.5

Als erstes öffnst du den Firefox Netzbetrachter, gehst auf Extras und klickst dann auf Add-ons.

Es hat sich nun der Add-ons-Manager geöffnet und du gibst in das Suchfeld Bloody Vikings ein und bestätigst mit Enter.

An der ersten Stelle ist auch schon das gesuchte Add-on. Nach einem Klick auf Installieren läd Firefox das kleine Helferlein herunter und installiert es.

Nach der Installation muss der Firefox Netzbetrachter neu gestartet werden damit das Add-on aktiv wird.

In Zukunft kann man in jedem Anmeldeformular mit der rechten Maustaste auf das Eingabefeld der eBrief Adresse klicken und aus dem Kontextmenü den Punkt „Bloody Vikings“ wählen.

Es wird in einem neuen Browser Tab die Webseite des Anbieters geöffnet und die temporäre eBrief Adresse in das Formularfeld eingetragen. Nach dem Absenden des Anmeldeformular wechselt man in den neu geöffneten Browser Tab und wartet auf die Bestätigungsmail.

Bitte beachte, dass einige Anbieter Cookies oder/und Javascript erfordern. Die nötigen Freigaben müssen vor der Nutzung konfiguriert werden.

8.46 User Agent Switcher

Das Add-On „User Agent Switcher“ ändert die Netzbertrachterkennung. Beim Aufruf einer Weltnetzseite identifiziert dich derssen Betreiber unter anderem mit deinem Netzbetrachternamen. Wenn du diese Angaben manipulieren willst, etwa um eine sog. „Browser-Sperre“ zu umgehen oder sich als jemand anderes auszugeben, benötigst du ein Spezialtool wie den „User Agent Switcher“.

Hier gezeigte Programmversion: 0.5.5

Als erstes öffnst du den Firefox Netzbetrachter, gehst auf Extras und klickst dann auf Add-ons.

Es hat sich nun der Add-ons-Manager geöffnet und du gibst in das Suchfeld User Agent Switcher ein und bestätigst mit Enter.

An der ersten Stelle ist auch schon das gesuchte Add-on. Nach einem Klick auf Installieren läd Firefox das kleine Helferlein herunter und installiert es.

Nach der Installation muss der Firefox Netzbetrachter neu gestartet werden damit das Add-on aktiv wird.

8.47 Tracking (Verfolgung durch Webseiten) verhindern

Du wirst verfolgt, um deine Weltnetzseitenaufrufe auszuforschen und Profile über dich anzulegen. Datenkraken wie z.B. Google, speichern nicht nur beinahe jede Eingabe und jeden Klick bei der bewussten Nutzung der Google-Dienste, sondern verfolgen und speichern möglichst jeden mit technischen Tricks ausgeforschten Seitenabruf auch außerhalb der eigenen Dienste.

Schützt du dich nicht gegen solches Tracking, erleichterst du das Anlegen und den potenziellen Missbrauch von sehr umfangreichen Profilen zu deiner Person, Arbeit und/oder Institution. Große Datenkraken lieben kleine Kekse: Verräterische Cookies

Um dich dauerhaft verfolgen und eindeutig identifizieren zu können, vergeben solche Schnüffler dazu u.a. eine dir zugeordnete Nummer, die im Hintergrund in einem sogenannten Cookie auf deinem Computer gespeichert und bei jedem der weiteren Abrufe wieder an die Schnüffler übertragen wird und diesen damit auch unabhängig von den unter Umständen wechselnden IP-Adressen oder Internetzugängen mitzuteilen, wer was abruft und damit, welches Profil weiter gepflegt werden soll.

So können über Jahre hinweg alle Suchen und Seitenabrufe diesen eindeutigen Nummern zugeordnet werden. Diese Nummern können wiederum - z.B. durch im Laufe der Zeit erfolgte Logins, anhand bestimmter IP-Adressen, den Spuren auf deinem Computer oder bestimmter Suchen oder Verhaltensmuster - mit deiner Person in Verbindung gebracht werden.

Um dich also vor langfristigem Nachstellen zu schützen, solltest du:

Cookies mindestens bei jedem Beenden deines Browsers löschen lassen und Cookies auch nur den Seiten erlauben, die du gerade aufgerufen hast

sich auch vor ähnlich funktionierenden Flash-Cookies schützen

in viele Seiten eigebetetten und bei der Ausführung Daten sammelnde JavaScripts von Trackingdiensten wie Google-Analytics blocken

Du erreichst dies z.B. mit folgenden Einstellungen:

Cookies vom Netzbetrachter löschen lassen
Flash-Cookies und Super-Cookies löschen lassen
Seitenübergreifende Dienste
Fingerabdruck des Netzbetrachters

8.48 DNS Abfragen verschlüsseln mit DNSCrypt

Wie sicherlich jeder schon gehört hat, kann eine URI wie s-f-n.org nicht einfach aufgerufen werden, denn der Name muss erst in eine IP-Adresse aufgelöst werden. Dafür zuständig sind DNS Server. Dein Computer fragt also einen DNS-Server was für eine IP z.B. youtube.com hat. Dabei sind diese DNS Abfragen aber Standardmäßig unverschlüsselt. Das heißt jeder der deine Weltnetz-Verbindung mitliest sieht welche Weltnetzseiten du besuchst.

Was macht DNSCrypt?

DNSCrypt setzt genau an diesem Problem an. Denn DNSCrypt verschlüsselt den DNS-Traffic. Also jene Antworten die normalerweise im Klartext übermittelt werden. Gleichzeitig laufen die DNS-Abfragen über den Port 443 per UDP. Dadurch kann der ISP (dein Internetprovider) weder Protokollieren auf welchen Seiten die Benutzer gewesen sind (Verschlüsselung), noch kann er andere DNS-Server blockieren. Außerdem werden so DNS-Filter umgangen.

DNSCrypt in der Praxis

Hier eine Demonstration einer DNS-Abfrage ohne DNSCrypt:

Auf dem Bild kannst du sehen dass die Antwort des DNS-Server im Klartext vorliegt. Sowohl IP Adresse als auch „youtube.com“ sind klar zu erkennen.

Mit DNS Crypt ist von der gut lesbaren Antwort nicht mehr viel übrig geblieben:

Einzigster Kritikpunkt ist, dass der DNS-Server in den USA steht. Nun muss jeder für sich ausmachen ob er dem Serverbetreiber vertrauen schenkt .. oder auch nicht.

Verwendung von DNSCrypt

Um DNSCrypt zu verwenden startest du zuerst die .exe Anwendung in „dnscrypt-win-client-master/DNSCrypt“. Als letztes musst du deinen DNS-Server in den Windows Einstellungen ändern.

Wie das funktioniert haben wir schon in einem anderen Artikel beschrieben. ≫ Wichtige Einstellungen für deinen Firefox

8.49 Firefox Portable

Ein Portable Browser ist wie der Name schon sagt, ein Netzbetrachter der nicht installiert werden muss. Dieser lässt sich direkt starten, und verarbeitet alles in einem einzigen Ordner. So könnte man diesen jetzt einfach auf einen USB Stick packen, und direkt von da aus starten. Hat man nun seine Arbeit im Weltnetz erledigt, kann man den Portable Ordner einfach mit Eraser sicher löschen, und den Stick zusätzlich noch formatieren. Somit sind alle Daten für immer vernichtet. Diese Methode schützt dich nicht vor dem Auslesen deiner IP Adresse sondern verhindert nur das jemand der Zugriff auf deinen Computer hat, sehen kann auf welchen Weltnetzseiten du dich

rumtreibst.

Wer keinen USB Stick zur Hand hat, kann auch eine Externe Festplatte nehmen, oder direkt vom Computer aus starten.

Noch eine Anmerkung. Firefox Portable sollte auch angepasst (siehe: Wichtige Einstellungen für deinen Firefox) werden und mit Plugins, bzw. Add-Ons versehen werden. Dazu lädst du dir den Netzbetrachter einfach runter, entpacke ihn, stellst alles ein wie du es haben willst, und installierst ganz normal die Erweiterungen.

8.50 Schutz vor Spionage- und Werbesoftware

Neben der Gefahr von Viren, Würmern, Trojanern und den menschlichen Hackern an sich, gibt es auch noch die Bedrohung durch Werbe-(Adware) und Spionagesoftware (Spyware). Während ersteres, ausgeschrieben „Advertising ware“ Werbungsprogramme, eher harmlos aber sehr nervig ist, solltest du letzteres doch ernster nehmen, denn dabei geht es konkret um die Spionage deiner Daten.

Durch installierte Spy- oder Adware öffnen sich aus dem Nichts sogenannte Popups, kleine Internet-Explorer Fenster (da dieser integrierter Bestandteil von Microsoft Windows ist), die eben Werbung für Pokerfreunde, Finanz- oder Potenzschwache oder eben deine Vorlieben oder Schwächen anzeigt. Möglich ist auch, dass die ungewollt installierten Programme sich eben nicht bemerkbar machen und lediglich im Hintergrund Daten an einen anderen fest bestimmten Rechner senden.

Diese Art von Programmen dient dazu, dein Verhalten im Netz zu protokollieren, die Daten später weiterzugeben um sie kommerziell nutzen zu können und entweder durch gezielte Werbung oder sonstige Zwecke zu verarbeiten.

Doch es gibt natürlich Abhilfe in Form von zwei Suchprogrammen, zum einen Spybot Search & Destroy von Patrick M. Kolla und zum anderen Ad-Aware von Lavasoft, zu welchen hier die Installationsanleitung gezeigt wird.

8.51 Spybot S&D und Ad-Aware

Dieser Leitfaden ist nicht mehr auf dem neusten Stand! Wir werden ihn so schnell wie möglich erneuern.

Falls Du evtl. die kostenpflichtige Version von Ad-aware benutzt und die eine Wächterfunktion besitzen sollte, würde ich nur eines der beiden Programme mit aktiver Wächterfunktion laufen lassen, denn Spybot bringt mit dem Tea Timer auch eine solche mit. Mehrere Wächterfunktionen gleichzeitig könnten sich gegenseitig ins Gehege kommen.

Benutzt du nur die kostenfreien Versionen der Programme, wie wir es in dem Leitfaden beschreiben, empfehlen wir dir beide Programme zu Installieren. Spybot S&D

Hier gezeigte Programmversion: 1.6.0.30

Zuerst lädst du dir die neuste Version von Spybot S&D herunter.

Nachdem du auf der Seite die neuste Installationsdatei heruntergeladen hast, öffnest du selbige mit einem Doppelklick und wählst bei der Sprache logischerweise Deutsch.

Im nächsten Fenster einmal auf Weiter gedrückt und die Lizenzvereinbarung durch Auswählen und nochmaliges Weiter bestätigt, kannst du nun den Ort angeben, an dem das Programm gespeichert werden soll. Am Besten alles so belassen wie es ist und Weiter.

Jetzt wählst du Komplette Installation. Nach weiterem dreimaligen Drücken des Weiter-Knopfes drückst du nun auf Installieren.

Das Installationsprogramm lädt sich jetzt die allerneuste Datei aus dem Weltnetz und installiert diese.

Ist die Installation fertig wählst du lediglich den obersten angebotenen Punkt – Spybot S&D starten – durch ein Häkchen aus und bestätigst.

Das Programm startet nun und gibt den Hinweis, dass du Programme die dich mit toller Spyware beehrten, womöglich nach einer Bereinigung durch Spybot S&D nichtmehr nutzbar sind – geht in Ordnung, weiter!

Die Bedienung des Programms geht nun herzlich einfach. Im Hauptfenster Überprüfen wählen und schon durchsucht das Programm die Datenträger nach dem „Dreck". Da es nach den unterschiedlichsten Arten solcher Software sucht (Malware, Hijacker, Trojaner, Dialer, ...) und sich die Zahl stets erhöht, kann die Suche schon einige Zeit, abhängig von der Prozessorgeschwindigkeit, dauern. Ist der Suchvorgang abgeschlossen, kannst du die gefundenen Werbeprogramme durch Markierte Probleme beheben löschen und dein System von ihnen bereinigen. Ad-Aware

Hier gezeigte Programmversion: 9.0.7

Zuerst lädst du dir die neuste Version von Ad-Aware herunter.

Ein Doppelklick auf die Installationsdatei und das Setup startet, hier wählst du direkt die Sprache DEUTSCH.

Du akzeptierst die Lizenzvereinbarung und drückst auf Installieren. Die Installation startet.

Ist die Installation beendet entfernst du das Häckchen um imformiert zu werden und musst somit keine E-Post Adresse angeben. Fertig stellen.

Nun öffnet sich der Update Managerund läd die neuste Software herunter.

Wenn das Programm gestartet ist, drückst du auf Jetzt scannen ¿ Vollständiger Scan und anschließend auf Scannen um das System komplett zu durchsuchen.

8.52 Virenschutz

Viren sind seit über 20 Jahren ein fester Begriff in der Welt des Internets. Neuer, aber nicht weniger gefährlich sind Würmer und Trojanische Perde (Trojaner). Die Gefahr, die von den kleinen Schädlingen ausgeht, wird aber leider immer noch von vielen Computer-Besitzern unterschätzt. Dabei ist es weder schwer noch teuer, sich vor Ungeziefer aus dem Netz zu schützen. Dieses Kapitel zeigt, was jeder Computer-Besitzer über Viren, Trojaner, Würmer und Co wissen sollte.

Mit diesen Schadprogrammen musst du rechnen, sobald du deinen Computer mit dem Internet verbindest:

Art	Risiko	Verbreitung	Schutz möglich
Viren	mittel	mittel	ja
Würmer	sehr groß	sehr hoch	ja
Trojaner	sehr groß	hoch	eingeschränkt
Hoaxes	mittel	mittel	eingeschränkt

Was also ist für dich zu tun wenn du keine Viren u.ä. auf deinem Computer haben möchtest?

8.53 Computerviren

Der Natur in die Karten geschaut: Die Bezeichnung „Viren“ stammt aus der Biologie. Zum tristen Alltag der unwillkommenen Besucher gehört es, unschuldige Zellen zu überfallen. Dafür besitzen Sie eine dünne Proteinhülle mit einem Nukleinsäurefaden. Dieser DNS-Strang enthält die Erbinformation des Virus, sein Programm. Bei den Bakteriophagen, die zu den höchstentwickelten Virenarten gehören, bohrt ein geschickt konstruierter Viruskörper ein Loch in die Hülle einer Opferzelle und injiziert seine DNS hinein.

Die Wirtszelle kann nur selten die eigenen Erbinformationen von den fremden unterscheiden. So befolgt sie sklavisch die in der Viren-DNS enthaltenen Anweisungen, und die sind eindeutig: Stelle exakte Kopien der viralen DNS-Stränge her und baue aus strukturalen Proteinen neue Körper für diese Viren-DNS auf.

Die infizierte Zelle produziert daraufhin eine wahre Armee von Viren. Am Ende eines Zyklus platzt die befallene Zelle wegen Überfüllung und entlässt Heerscharen von Viren in die Umgebung. Die Wirtszelle stirbt, und die von ihr produzierten Erreger dagegen starten einen neuen Kreislauf.

Im Computer läuft das Spiel des Lebens fast genauso ab: Die Programme in deinem Computer sind nichts weiter als Anweisungen, jedes ein Papierstapel, auf dessen Seiten Befehle für den Prozessor stehen. Die CPU arbeitet die Programme Seite für Seite ab, wartet auf Eingaben oder springt zu anderen Seiten im Stapel, um deren Befehle auszuführen.

Computerviren erweitern diese Stapel mit neuen Seiten, Ersatz-Anweisungen. Da Programme und CPU sich ihrer selbst nicht bewusst sind, führen sie stur aus, was auf den neuen Seiten steht: Wie man neue Viren herstellt.

Ein so geändertes Programm gilt als „infiziert“. Es kann möglicherweise (nicht immer) noch alles tun, wozu es ursprünglich gedacht war, aber es tut eben auch zusätzliche Dinge und gilt deswegen als gestört. Je nach Infektion ist es sogar beschädigt, weil der Virus ein paar den alten Seiten wegschmiss, um Platz für seine eigenen Seiten zu schaffen - dann stürzt das Programm unerwartet ab.

Virus-Aufbau: Körper, Sprengkopf, Zünder

Viren unterscheiden sich von anderen Programmanomalien (Würmer, Trojaner) vor allem dadurch, dass sie nicht für sich selbst existieren können. Stets benötigen sie ein Wirtsprogramm, die sie befallen können. Sie bestehen grob gesprochen aus vier Teilen:

Aktivierung: Der Virus muss die Kontrolle über das System erlangen, also mindestens einmal pro Neustart aufgerufen werden. Der Code des Virus-Aufrufs kann sich an einer ganz anderen Stelle befinden als der Viruskörper selbst. Vermehrung: Die Fortpflanzungs-Komponente des Virus hält Ausschau nach Programmen, die als Opfer in Frage kommen. Sind passende Wirte entdeckt, infiziert es sie, wobei es bestimmte Regeln einhält, um optimal zu arbeiten. Wirkung: Die Nutzlast, im Virenforscher-Slang oft „Payload“ genannt, ist eine harmlose oder gefährliche Wirkung. Sie wird über einen Auslöser („Trigger“) aktiviert, der prüft, ob definierte Bedingungen vorliegen.

Tarnung: Eine Tarn-Komponente sorgt dafür, dass der Virus von Anwendern und Antivirenprogrammen nicht entdeckt wird.

Ein unschuldiges, gesundes Programm sieht ungefähr so aus:

Anfang
Anweisung 1
Anweisung 2
Anweisung 3
Ende

Dieses Opferlamm wird nun durch den Wunschzettel der Viren-Macher erweitert: Der Virus soll aktiviert werden, sobald sein Wirt aktiviert wird; er soll Dateien erkennen, die er problemlos infizieren kann; er soll sich dann in diese Dateien hineinkopieren und sich vermehren; die Kopie soll dabei identisch sein, damit sie weiterhin funktioniert; der Virus soll sich dabei verstecken oder wenigstens nicht auffallen; er zusätzlich zu bestimmten Zeitpunkten eine Wirkung haben.

Das sieht dann grob so aus:

Anfang
Virus-Anfang (Aktivierung)
Virus-Tarnung
Virus-Vermehrung
Virus-Wirkung
Virus-Ende
Alter Anfang
Anweisung 1
Anweisung 2
Anweisung 3
Altes Ende

Wie du siehst: Viren sind kein Hexenwerk!

Sind Viren heute noch ein Problem?

Es geht so, eher nein. Die meisten der Dinge, die wir heute „Viren“ nennen und die von „Virenscannern“ gejagt werden, sind in Wirklichkeit Trojaner und Würmer. Aber mit den Viren hat vor dem Netzwerkzeitalter alles angefangen.

-Computerwürmer, die Nachfolger der Computerviren

Erreger geistern durchs Netz: Viren sind geradezu harmlose Tierchen, denn sie nehmen sich nur eine oder mehrere Dateien vor und infizieren diese. Computerwürmer dagegen wollen immer gleich alles: Sie infizieren nicht einzelne Dateien, sondern das gesamte Computersystem, am besten auch gleich alle anderen Computer, die mit dem Opfer irgendwie verbunden sind.

Generell gehört es also zum wurmhaften Verhalten, ein Netzwerk zu infizieren - der Befall eines einzelnen Systems ist nur ein Mittel zum Zweck, andere Systeme zu erreichen. Einige Würmer entfernen sich selbst wieder aus dem System (oder sollen es nach Plan ihrer Schöpfer tun, es geht aber manchmal schief). In diesem Fall „reist“ die Software-Anomalie durch das Netz von Rechner zu Rechner, ohne sich an einem bestimmten Ort lange aufzuhalten. Das hört sich ein bisschen abstrakt an und ist es auch, und wohl deswegen werden die meisten Würmer heute einfach als Viren bezeichnet. In Wirklichkeit ist es heute aber umgekehrt: Die meisten Viren sind heute genau

genommen eigentlich Würmer.

Kettenbriefe und E-Mail-Würmer

Die frühen E-Mail-Programme auf Hostrechnern besaßen die Fähigkeit, mit Script-Programmiersprachen kleine Tools auszuführen - man konnte sozusagen seine E-Mail-Software „programmieren“. Das hatte schon früh zur Folge, dass einige Spaßvogel Briefe schrieben, deren einzige Funktion es war, sich selbst zu reproduzieren und an weitere Nutzer zu verschicken. Als Nachfolger dieser automatischen E-Kettenbriefe können heute alle Viren und Würmer gelten, die sich über Microsoft Outlook verbreiten. Der Wurm lebt dabei meistens in einem ausführbaren Anhang (Programme, Scripte) und benötigt zu seiner Vermehrung ein Mailprogramm, um dessen Netzwerkfunktionen zu nutzen.

Würmer mit Viren- und Trojaner-Techniken

Die neuen Würmer stellen die derzeit größte Gefahr dar, denn sie kombinieren auf teuflische Weise alle bisher bekannten Möglichkeiten von Software-Anomalien:

Sie setzen auf rasche Ausbreitung durch Wurm-Techniken, indem sie Mailprogramme oder Netzwerke benutzen, um andere Computer anzustecken.

Sie infizieren Dateien und Dokumente, um den Computer „als Ganzes“ zu unterwandern. Sie besitzen Schadensfunktionen, wie sie sonst für Viren typisch sind. („Normale Würmer“ verzichten darauf, denn sie wollen nicht auffallen.)

Sie hinterlassen Trojanische Pferde und Keylogger in Windows, um Passwörter zu stehlen oder den Nutzer zu belauschen.

E-Post und Internet sind derzeit die gefährlichsten Quellen, denn sie sind das das Medium schlechthin für jeden Wurm.

Schon 2001 hatte sich nach Angaben von Kaspersky Labs die Zahl der Viren-Angriffe per Mail im Vergleich zum Vorjahr um etwa fünf Prozent erhöht und soll nun schon 90 Prozent aller Virenvorfälle ausmachen. Und alternative Infektionskanäle wie ICQ, Gnutella, MSN Messenger oder IRC werden gerade erst von den Wurm-Machern als neues Spielfeld entdeckt, ebenso neue Plattformen wie Linux.

Inzwischen gibt es so viele Würmer auf dem Computer, dass man sie in verschiedene Typen aufteilen kann. Die Trennung erfolgt dabei vor allem nach den Einfallschneisen, über die Würmer unsere Computer infiltieren, und nach den Techniken, die sie einsetzen.

Dateileichen pflastern ihren Weg

Script-Würmer: Damit sind alle Würmer gemeint, die aus Anwendungs-Makros bestehen und zum Beispiel aus Word heraus Outlook und andere Microsoft-Produkte fernsteuern, oder Würmer wie Loveletter, die aus einem alleinstehenden Visual Basic Script (VBS) bestehen. Die meisten Wurm-Epidemien gehen auf das Konto der VB-Scripte, da Outlook in einigen Versionen Scripte schon ausführt, wenn man nur die Mails anzeigt, welche die Scripte enthalten.

File-Würmer: Obwohl VBS als Wurm-Faktor Nummer 1 gilt, gibt es auch Würmer, die sich ohne jedes Script ausbreiten. Hier besteht der Wurm aus einem ganz ordinären Programm. In Form eines Virus kann es Dateien infizieren und so dem PC einen Wurm verpassen. Viel öfter aber verankert sich der Wurm als zusätzliches Programm im System, fast wie ein Gerätetreiber. Der Nutzer installiert ihn sich normalerweise über ein Trojanisches Pferd, indem er unvorsichtigerweise auf

einen Dateianhang klickt, zum Beispiel der angebliche Screensaver, in dem der Goner-Wurm steckt.

IRC-Würmer: Der Internet Relay Chat (IRC) ist ohnehin schon ein Tummelplatz für alle Nutzer mit leicht kriminellen Neigungen, doch wegen gewisser Eigenheiten haben sich dort auch scriptfähige IRC-Clients durchgesetzt, allen voran mIRC. Diese Scripts könnten im Prinzip nützlich sein, doch man kann mit ihnen auch Nutzer aus dem Chat drängen oder ihre Clients „abschießen“ - schon vor Jahren bildete sich eine eigene Szene mit Kampf-Scripts, die sich gegenseitig in Schach hielten. Inzwischen gibt es zahlreiche Würmer und Viren, die in der Lage sind, auch IRC als Ausbreitungsweg zu verwenden, indem sie sich die Scripte untertan machen.

IM-Würmer: Ob ICQ, AOL Instant Messenger (AIM) oder Microsoft Messenger - immer wieder fallen die Instant Messenger (IMs) durch Sicherheitslücken auf. Und als wäre das nicht genug, versucht eine neue Wurm-Generation, die IMs zur Ausbreitung zu benutzen. Und es ist einfach: Die IM-Würmer verschicken einfach eine Kurznachricht mit Datei an die im IM eingetragenen Freunde (Buddy-List). Prinzipiell funktionieren sie also wie Würmer, die sich per Mail verbreiten.

...und viele weitere mehr, sowie:

Dropper und Construction Kits: Viren und Trojanische Pferde können auch dazu dienen, einen Wurm in deinem System abzuwerfen. Darüber hinaus gibt es inzwischen schon eigene Wurm-Generatoren, also Software, mit deren Hilfe sich jeder in wenigen Sekunden einen eigenen Wurm zusammenklicken kann.

8.54 Trojaner

Trojaner werden gerne in einer Reihe mit Viren und Würmern genannt. Und tatsächlich gehören die so genannten Trojanischen Pferde durchaus zu den Programmen (im Fachjargon Malware genannt), die enormen Schaden anrichten können. Allerdings sind Trojaner nicht unmittelbar schädlich - im Gegensatz zu Viren legen sie beispielsweise nicht den Computer lahm. Ihre Schadensroutine reicht viel weiter - und ist weitaus perfider als die von Viren.

So arbeiten Trojaner

Der Begriff Trojanisches Pferd geht auf den griechischen Dichter Homer zurück. In seiner „Ilias“ berichtet Homer von griechischen Kriegern, die sich bei der Belagerung der Stadt Troja in einem hölzernen Pferd versteckten. Die Einwohner Trojas glaubten an ein Geschenk und brachten das Holzpferd in ihre Stadt. Nachts schlüpften die griechischen Krieger aus dem Pferd und öffneten von innen die Stadttore um ihre Kameraden hereinzulassen. Damit war die Schlacht für Troja verloren. Ähnlichen arbeiten Trojanische Pferde in der Computerwelt: Sie verstecken sich in scheinbar nützlichen Programmen, gelangen so unbemerkt auf den Computer und beginnen dann damit, Schaden anzurichten oder schädliche Komponenten aus dem Internet nachzuladen. Auch deshalb werden Trojaner von vielen Antivirenprogrammen als Trojan-Downloader bezeichnet oder erkannt. Im Gegensatz zu Viren oder Würmern verbreiten sich Trojaner in der Regel nicht fort und reproduzieren sich auch nicht selbst.

Die Schadensroutinen bei Trojanischen Pferden können sehr unterschiedlich sein. Daher sollen an dieser Stelle nur die Wichtigsten genannt werden:

- Die meisten Trojaner sind darauf programmiert, auf dem infizierten Rechner Daten zu sammeln, angefangen von Passworten und Kreditkartennummern bis hin zu Eingaben über die Tastatur. Diese Daten können dann über das Internet an den „Lenker“ des Trojaners über-

mittelt werden. Programme, die die Tastatureingaben aufzeichnen, nennt man auch Keylogger.

- Mindestens ebenso gefährlich sind die so genannten „Server-Programme“. Hast du dir erst einen Trojaner dieser Art eingefangen, kann ein anderer Nutzer online auf deinen Computer zugreifen, ihn steuern und ihm bestimmte Befehle geben. Um dies möglich zu machen, öffnet der Trojaner am befallenen Rechner bestimmte Ports. Ports sind vergleichbar mit Eingangstüren zum Internet. Durch diese offenen Ports hat der Trojaner-Lenker dann Zugriff.
- Trojan-Downloader sind - wie oben schon geschildert - kleine Programme, die sich auf einem Computer einnisten und dann von sich aus bei passender Gelegenheit weitere schädliche Programme nachladen. Zu diesen nachgeladenen Komponenten gehörten in der Vergangenheit oftmals teure 0900-Dialer, also Einwählprogramme, die den Rechner des Betroffenen über eine hochtarifierte Telefonnummer mit dem Internet verbinden. Dies geschah in vielen Fällen unbemerkt vom Betroffen.
- Werbe-Trojaner sind darauf programmiert, Nutzer mit unerwünschter Werbung zu „bombadieren“, teure 0900-Dialer zu installieren oder Betroffene auf entsprechende Seiten zu entführen.

Trojaner sind oft so programmiert, dass sie automatisch mit dem Betriebssystem starten. Sie laufen also automatisch im Hintergrund mit, was die Entfernung für den unerfahrenen Computer-Nutzer sehr schwierig macht. Andere Trojanische Pferde starten erst, wenn der Nutzer auf ein bestimmtes Programm auf den Rechner zugreift.

Cracker nutzen bestimmte Programme („Port-Scanner“), um im Internet nach Rechnern zu suchen, die von einem Trojaner befallen sind. Diese Scans bemerkt man in der Regel nur durch eine Firewall, die solche Zugriffsversuche aufzeichnet.

8.55 Hoaxes, Kettenbriefe und falsche Warnungen

Das Wort „Hoax“ stammt aus dem Englischen und geht auf eine alte Tradition bei Hofe zurück. Damals machten sich die Adeligen einen Spaß daraus, falsche Gerüchte zu verbreiten und amüsierten sich dann köstlich darüber, wenn ihr Gegenüber darauf hereinfiel. Heute versteht man unter Hoaxes vor allem falsche Virenwarnungen und Gerüchte, die per ePost gestreut werden.

Von der falschen Virenwarnung über Aufrufe zu Knochenmarkspenden bis hin zur angeblichen Petition, um einen chinesischen Bären zu retten: Im Internet werden die kuriosesten Meldungen und Behauptungen per Mail gestreut. Von harmlosen Scherzen sind Hoaxes allerdings weit entfernt. Im Gegenteil: Sehr oft richten sie auch direkten oder indirekten Schaden an.

Fallbeispiele:

- Immer wieder kursiert zum Beispiel die Falschmeldung, die GEZ (Gebühreneinzugszentrale der Rundfunkanstalten) würde rückwirkend Rundfunkgebühren zurückerstatten. Grund sei ein entsprechendes Urteil des OLG Augsburg. Fakt ist: Ein Oberlandesgericht (OLG) Augsburg gibt es überhaupt nicht. Die GEZ allerdings wird dann Dank des Hoaxes von Tausenden Anfragen überhäuft.
- Ebenfalls nicht tot zu bekommen: Die per ePost verbreitete Warnung, in Discotheken oder in Kinos wären Besucher von einem Unbekannten durch einen Nadelstich mit dem HI-Virus infiziert worden. Die regelmäßige Folge: Verunsicherung, Arbeit für die Polizei, die dem Gerücht nachgehen muss, finanzieller Schaden für die angeblich betroffenen Einrichtungen.

- Schon seit 1999 kursiert eine Email, nach der Microsoft-Gründer Bill Gates zu einem Mail-Beta-Test aufgerufen habe und Microsoft für die einfache Weiterleitung von Mails bestimmte Geldprämien vergebe. Der Gates-Kettenbrief wird alle paar Monate wieder zu neuem Leben erweckt - und findet dabei immer wieder Dumme, die auf ihn hereinfallen und ihn weiterverbreiten.

- Seit 2003 wird die Warnung verbreitet, auf dem Mobiltelefon könne ein Änruf in Abwesenheitërscheinen, der von einer Telefonnummer „+49137799090269" (oder ähnlich) stammt. Wer die Nummer zurück rufe, lande in der Kostenfalle: Die Verbindung werde bis zu einer Stunde gehalten und man könne die Verbindung selbst nicht beenden, womit enorme Kosten anfielen. Bisweilen beruft sich die ePost dabei auf eine Quelle bei der Polizei oder einem Landeskriminalamt. An diesem Kettenbrief zeigt sich das eigentlich Perfide an Hoaxes: Die Nachricht beruht zu einem kleinen Teil auf wahren Ereignissen, die allerdings verfälscht werden. Denn betrügerische Lockanrufe mit 0137-Nummern gibt es tatsächlich; wer zurückruft, zahlt jedoch „nur" einen Pauschalbetrag von bis zu zwei Euro. Dass die Verbindung bis zu einer Stunde gehalten werde, ist dagegen falsch.

Hoaxes klingen zumeist sehr ernst, zumal sie sich oft auch auf renommierte Unternehmen und Stellen berufen - freilich ohne deren Wissen und Zutun.

Wer dubiose Warnungen, Aufforderungen oder andere Hoaxes unaufgefordert per ePost erhält, tut also gut daran, diese entweder nicht ernst zu nehmen oder auf renommierten Seiten - etwa bekannten Antiviren-Seiten - zu verifizieren.

Ganz wichtig:
Man sollte es unterlassen, derartige Falschmeldungen selbst weiter zu verbreiten. Nicht nur, dass man damit sonst dem Urheber einen Gefallen tun, Bandbreite verschwendet und zur weiteren Vermüllung des Internets beiträgt - man gerät auch schnell in den Verdacht, ein naiver „DAU" (steht für „dümmster anzunehmender User") zu sein, der auf alles hereinfällt.

8.56 Schutz vor Viren, Trojanern und Würmern

Jeden Tag werden mehr als hundert neue Viren, Trojaner und Würmer ins Netz geschleust. Insgesamt sind derzeit weit über 50 000 verschiedene Schädlinge und deren Unterarten bekannt - zumal es in der „Szene" mittlerweile zu einem regelrechten Sport geworden ist, immer neue, noch gefährlichere Schadprogramme zu entwickeln. Dennoch ist man dieser Entwicklung nicht schutzlos ausgeliefert, wenn man ein paar Regeln beachtet. Seie misstrauisch bei ePost

Viren und Trojaner werden heutzutage vor allem durch eMails verbreitet. Dass eine Mail gefährliche Inhalte transportiert, erkennst du an folgenden Indizien:

- Die ePost kommt von einem dir unbekannten (ausländischen) Absender
- Der Betreff der ePost ist sinnlos (etwa „Hi", „Re: Document", „Your Mai"...)
- Die ePost enthält keinen Text, sondern nur einen Anhang
- Du wirst in der ePost dringend aufgefordert, auf den Anhang zu klicken
- Der Anhang einer ePost enthält ausführbare Programme.
- Dies erkennst du unter Umständen an der Dateieindung (exe,com,pif,scr,cmd,vbs,vxd,chm).
- Anhänge mit diesen Buchstaben am Ende des Dateinamens sind mit höchster Wahrscheinlichkeit gefährlich und sollten niemals geöffnet werden.

Virenmails mit deinem Absender?

Möglicherweise wirst du eines Tages von einem dir unbekannten Menschen mit dem Vorwurf konfrontiert, du hättest ihm eine virenverseuchte ePost zugeschickt. Dafür gibt es eine einfache Erklärung: Moderne Viren und Würmer sind so programmiert, dass sie sich selbst im Weltnetz verbreiten. Dafür besorgen sie sich die Adressen, an die sie sich versenden, selbst, etwa in öffentlichen Gästebüchern, in Newsgroups, auf Webseiten - und in den Adressbüchern auf bereits infizierten Rechnern. Bei dem genannten Szenario kann es also passieren, dass ein Wurm oder Virus ausgerechnet deine Mailadresse findet und sich unter diesem Namen weiterversendet.

Wenn du entsprechende Meldungen oder Beschwerden erhältst, kläre den Beschwerdeführer über diese Eigenschaft von Schadprogrammen auf. Überprüfen deinen eigenen Rechner aber trotzdem mit einem aktuellen Virenscanner. Es ist niemals auszuschließen, dass dein Computer ebenfalls bereits infiziert ist.

Trojaner und Viren in Tauschbörsen

Tauschbörsen wie Emule sind für Programmierer von schädlichen Programmen ein optimaler Platz, um Viren, Trojaner oder Würmer in Umlauf zu bringen. Insofern gilt auch hier höchste Aufmerksamkeit. Denn statt des vermeintlichen Films, Programms oder Musikstücks kannst du dir auch gefährliche Malware einfangen. Wer unbedingt Tauschbörsen nutzen will, sollte heruntergeladene Dateien immer (!) vor dem ersten Start mit einem Virenschutzprogramm überprüfen.

Virenschutz installieren
Ohne Antivirus- und Trojanerschutz-Programm sollte heute niemand mehr im Internet unterwegs sein. Auf der nächsten Seite findest du das Antivirus Programm: Avira AntiVir Personal Free

8.57 Avira AntiVir Personal Free

Ein empfehlenswerter und dazu noch kostenloser Virenscanner ist die Personal Free Version von Avira.

Hier gezeigte Programmversion: 13.0.0.2890

Zuerst lädst du die neuste Version von Avira AntiVir Personal Free herunter.

Nachdem du die Datei heruntergeladen hast, öffnst du sie mit einem Doppelklick und der Installationsvorgang sollte starten. Weiter gehts mit einem klick auf Express und hier musst du die Lizenzvereinbarung akzeptieren. Weiter.

Nun wird AntiVir installiert. Ist die Installation fertig klickst du auf Fertig stellen.

Das Programm startet jetzt selbstständig und läd wichtige Updates herunter. In der Regel sind es bei einer Neuinstallation von AntiVir mehrere MB. Je nachdem, wie schnell deine Verbindung ist, dauert es nun ein paar Minuten und das Programm und seine Virendatenbank sind auf dem aktuellsten Stand.

Als nächstes prüft AnriVir das komplette System automatisch. Dieses kann je nach Größe der Festplatte einige Minuten dauern.

Wenn dies beendet ist wird dir ein Bericht gezeigt der im besten Falle so aussehen sollte. Keine Warnungen, Verschiebungen, Löschungen u.s.w. . Nun drückst du auf Close.

Avira AntiVir Personal Free ist nun installiert und läuft bei jedem Start des Rechners im Hintergrund mit, um jede Datei die du öffnest zu überprüfen. Ist eine Datei verdächtig oder hat sich ein Virus bei dir eingenistet, schlägt das Programm Alarm und bietet dir an ihn zu löschen oder zu belassen.

Willst du einen Datenträger, z.B. eine CD, ein USB-Speicherstick oder eben eine Festplatte komplett überprüfen, drückst du rechts unten in der Systemtray auf den weißen Schirm auf rotem Hintergrund und die Hauptoberfläche öffnet sich. Du drückst nun oben auf den Karteireiter Prüfen und kannst das jeweilige Speichermedium auswählen. Dann noch links oben auf die Lupe gedrückt und der Suchvorgang mit Namen Luke Filewalker startet.

Um stets den bestmöglichen Schutz vor Viren etc. zu haben, empfehlen wir den Virenscanner mindestens ein-bis zweimal im Monat, besser alle zwei Tage zu aktualisieren!

8.58 Weltnetz - Verläufe löschen

Sei es am Arbeitsplatz, zuhause oder bei einem Bekannten, für neugierige Zeitgenossen ist es leicht ersichtlich, welche Adressen du im Weltnetz aufgesucht hast; vorausgesetzt sie haben Zugriff auf den Computer, an dem du vorher durchs Web gesurft bist.

Sie müssen nur wissen, an welchen Stellen sie nachzuschauen haben. Vor allem der Verlauf (die History), der Cache (Pufferspeicher, temporäre Dateien) und die Cookies geben Aufschluss über deine Surfgewohnheiten. Vergessen solltest du natürlich auch nicht die sog. Bookmarks (Lesezeichen, Favoriten), falls du dort Adressen gespeichert hat, die nicht für fremde Augen bestimmt sind!

Natürlich ist es aber hier möglich diese Spuren zu verwischen. Das Programm cCleaner entfernt vor allem den Verlauf von besuchten Weltnetzseiten und diverse andere Verläufe, wie z.B. zuletzt benutzte Dateien oder eingegebene Suchbegriffe der Windows-Suche. Es ist auch möglich, unbenutzte und temporäre Dateien zu bereinigen.

8.59 Was wird vom cCleaner bereinigt?

Der cCleaner ist eine Allzweck-Waffe gegen Datenmüll. Je länger du mit Windows arbeitest, desto mehr Datenmüll bleibt auf der Festplatte zurück. Dieser stammt teilweise von Programmen, die nicht rückstandslos vom Computer entfernt wurden. Auch beim stöbern im Weltnetz sammelt sich eine Menge Balast an, von dem du deinen Computer befreien kannst.

Internet Explorer

Temporäre Dateien, Verlauf, Cookies, Autovervollständigung, index.dat-Dateien.
Firefox

Firefox

Temporäre Dateien, Verlauf, Cookies, Download-Verlauf, Formulardaten.
Google Chrome

Temporäre Dateien, Verlauf, Cookies, Download-Verlauf, Formulardaten.
Opera

Temporäre Dateien, Verlauf, Cookies, Download-Verlauf.

Apple Safari, Safari

Temporäre Dateien, Verlauf, Cookies, Formulardaten.
Weitere unterstützte Browser

K-Meleon, Rockmelt, Flock, Google Chrome Canary, Chromium, SeaMonkey, Chrome Plus, SR-Ware Iron, Pale Moon, Phoenix, Netscape Navigator, Avant und Maxthon.
Windows

Papierkorb, zuletzt geöffnete Dokumente, Temporäre Dateien, Logdateien, Zwischenablage, DNS Cache, Fehlerberichterstattung, Speicherabbilder, Jumplisten.
Registry

Registrierungsreiniger

Erweiterte Funktionen zum Entfernen von unbenutzten und alten Einträgen, Dateierweiterungen, ActiveX Controls, ClassIDs, ProgIDs, Deinstallationen, Bibliotheken, Schriften, Hilfedateien, Anwendungspfaden, Icons, ungültigen Verknüpfungen und mehr...
Applications

Anwendungen von Drittanbietern

Entfernt temporäre Dateien und zuletzt benutzte Dateilisten (MRUs) von vielen Anwendungen wie Windows Media Player, eMule, Google Toolbar, Microsoft Office, Nero, Adobe Acrobat, WinRAR, WinAce, WinZip und vielen anderen...

Du hast mit dem kostenlosen cCleaner jedoch mehr Möglichkeiten als nur den Datenmüll beseitigen. So kannst du z.B. auch die Autostart Einträge ändern oder die Systemwiederherstellungspunkte löschen. Hier bitte vorsichtig sein, denn gelöschte Einträge können nicht wiederhergestellt werden

Eine weitere sehr sinnvolle Funktion des Programmes ist die des „Freien Speicher sicher löschen“. Wenn die Funktion aktiviert wird, berechnet der cCleaner zunächst den verbleibenden Speicherplatz und erstellt dann eine Datei, die so groß ist. Diese schreibt er auf die Festplatte und löscht sie anschließend wieder. Somit werden alle alten Dateien, die zwar gelöscht sind, aber auf der Festplatte noch vorhanden und wiederherstellbar sind, überschrieben. Nach diesem Überschreiben kann man die Dateien nicht wiederherstellen. Eine Funktion, die sich wunderbar anbietet, wenn man z. B. den Computer verkaufen und sicher sein will, dass alle persönlichen Daten gelöscht und nicht wiederherstellbar sind. Das kann je nach Größe der Festplatte einige Zeit dauern.

cCleaner
Mythen und Klischees in der Informatik zu beseitigen, erinnert nicht selten an den Kampf von Don Quijote, wobei der Unterhaltungswert in einigen arg strapazierten Bereichen eher gen null tendiert und sich auch eine gewisse Ermüdung breit macht, wenn es darum geht, ständig den gleichen Unsinn zu revidieren. Das soll uns nicht davon abhalten, noch einmal das Thema Datenmüll-Bereinigung und Registry Cleaner aufzugreifen, um vielleicht doch noch etwas mehr Skepsis bei dem Umgang mit diesen Tools zu erzeugen.

Um es ganz deutlich zu formulieren, in diesem Artikel geht es nicht um die Vorzüge von Registry Cleanern, sondern in erster Linie um den cCleaner, den wir nach wie vor für als sehr nützlichen Helfer beim Eliminieren von Datenmüll einstufen. Das Thema Registry Cleaner reflektieren wir in einem extra Kapitel gegen Ende dieser Anleitung, zu der wir dir viel Vergnügen und hoffentlich die richtigen Erkenntnisse wünschen...

Hier gezeigte Programmversion: v3.23.1823

Installation und wichtige Hinweise:

Um in den Genuß des cCleaners zu kommen, benötigst du natürlich den entsprechenden Download, eine 32 oder 64 bittige Unterscheidung gibts es weder für den Download noch für die Installation:

Nachdem du die Installationsdatei heruntergeladen hast, öffnest du sie mit einem Doppelklick. Achte bei der Installation bitte darauf, das du überflüssige Zusatzprogramme (speziell die Yahoo Toolbar oder Google Toolbar/Google Chrome) nicht mit installierst. Natürlich muß und will Piriform über dieses virale Marketing Geld verdienen, aber bitteschön nicht unbedingt gerade mit diesem Toolbar-Mist. Schließlich wollen wir die Datenmüllbeseitigung des cCleaners nicht dadurch konterkarieren, in dem wir quasi durch die Hintertür beispielsweise die Argusaugen des Suchmaschinen-Marktführers ins System zurückholen...

Während der Installation wirst du auch nach der Sprachversion gefragt, die du nach Gusto auswählen kannst, der cCleaner legt dir diesbezüglich kaum Steine in den Weg.

Auch die ganzen zusätzlichen Kontextmenüeinträge usw. sind absolut überflüssig (bitte den Screenshot beachten), weil sie nur zu Klicks verleiten, die eher an die Spontanität als Vernunft zu adressieren sind. Automatischen Updates sollte man grundsätzlich mit Skepsis gegenüberstehen, zumindest bei 3rd-party Software und zu denen gehört der cCleaner. Der Grund ist kausal, alles was in diesem Bereich aktiv ist, mischt sich in Systemressourcen ein, die nicht immer mit den hierarchischen Abfolgen eines Betriebssystems harmonieren!

Beim klick auf Fertig stellen ...

... öffnet sich ein Fenster in dem du gefragt wirst ob du nach nicht zu löschenden Cookies scannen möchtest. cCleaner möchte dir hier eine Hilfe sein und Coocies mit Passwortangaben nicht löschen. Da du aber keine Passwörter oder Benutzernamen auf deinem Computer gespeichert haben möchtest klickst du hier auf NEIN.

Wichtige und gefahrlose Einstellungen:

Wenn die Installation absolviert wurde und du den cCleaner das erste mal mit Adminrechten startest, geht es an die Einstellungen des cCleaners, für die wir dir entsprechende Screenshots angefertigt haben, damit du die gefahrlosesten Einstellungen übernehmen kannst. Unsere Einstellungen basieren auf Langzeiterfahrungen mit den Betriebssystemen Windows XP -¿ Vista und Windows 7, wobei die aktuelle Windows 8 Preview sich bisher analog dazu verhält. Vista- und Windows 7 Benutzer starten den cCleaner immer mit Rechtsklick auf das Symbol und wählen „Als Administrator ausführen“.

Die Begründung für diese Einstellungen liegen auf der Hand: Kennwörter sollten grundsätzlich nie gespeichert werden, egal in welchem Bereich sie angelegt wurden. Verknüpfungen werden von Windows Vista und auch Windows 7 anders kategorisiert als noch zu Zeiten von Windows XP, darum raten wir von deren Bereinigung ab. Dies gilt ebenso für tiefergreifende Systembereinigungen (ausgegraute Bereiche), bei denen schon eine zu viel gelöschte Datei ausreicht, um die ersten Probleme zu generieren.

Was im Karteireiter „Anwendungen“ bereinigt werden kann, hängt natürlich in erster Linie davon ab, was du an externen Programmen installiert hast. Grundsätzlich sind diesbezüglich aber kaum Systemirritationen zu erwarten, zumindest nicht vom Betriebssystem. Darüber hinaus ist der cCleaner mittlerweilse so ausgereift, das diesbezüglich relativ wenig Substanz für Fehlerquellen existieren. Solltest du allerdings Software verwenden, die in dieser Hinsicht anfällig reagiert,

kannst du jederzeit deren Optionshaken wieder entfernen.

Kurzum: Über diese nun klar definierte Reinigungsroutine kannst du deinen Computer gefahrlos z.B. nach jeder Internetsitzung oder Programminstallationen bereinigen, ohne das du sensible systemrelevante Bereiche tangiert. Selbstverständlich kannst du unsere Vorgabe auch nach Gusto ändern, wir haben so allerdings die besten Erfahrungen gemacht und unsere Prämisse hieß: möglichst gefahrlos und mit minimalem Risiko...!

apropos Risiko: Wir empfehlen ohnehin vor der ersten Systembereinigung mit dem cCleaner auf einem frisch eingerichteten System ein Image (Abbild) mit einer geeigneten Software zu erzeugen, damit du immer einen passenden Rettungsanker parat hast.

Den Karteireiter Registry ignorieren wir ganz bewußt (warum steht im separaten Kapitel) und widmen uns dem nächsten interessanten Punkt: der Button Extras:

Hier findest du insgesamt vier Untermenüs: Programme deinstallieren, Autostart, Systemwiederherstellung und Festplatten Wiper.

Programme lassen sich unter Windows Vista und Windows 7 mittlerweilse ausgezeichnet deinstallieren und falls nicht, hilft der cCleaner auch nicht entscheidend weiter, denn schlecht programmierte Deinstallationsroutinen lassen sich in der Regel von solchen Hilfsmaßnahmen wenig beeindrucken. Dies gilt ebenso für die Systemwiederherstellung, die ohnehin nur so gut funktioniert, wie Windows es zuläßt.
Festplatten Wiper (sicheres Löschen) von feierm Speicherplatz auf deinen Festplatten brauchst du eigentlich nicht solange du alle Daten sicher Löschst und nicht nur in den Papierkorb wirfst. Siehe: Dateien sicher löschen

Bliebe noch der Punkt Autostart, der in der Tat durchaus einige Ansätze bietet, um gezielt ins System einzugreifen, wenn msconfig an seine Grenzen stößt:

Die Möglichkeit störende Einträge nicht gleich zu löschen, sondern zunächst zu deaktivieren und bei Bedarf wieder zu aktivieren, ist sicher einer der Vorzüge in diesem Abschnitt des cCleaners, zumal er neben dem Windows Autostart zusätzlich noch den Internet Explorer und Scheduled Tasks (geplante Aufgaben) als erweiterte Optionen anbietet, da kann msconfig nicht mithalten. Aber auch hier gilt wieder, Hände weg von der Maus, wenn du nicht weißt was diese oder jene Einstellung bewirkt und lösche bitte nicht gleich die Autostarteinträge ! sondern bleibe maximal bei der Deaktivierung.

Kommen wir zum Optionsbutton Einstellungen:

Unter Einstellungen -¿ Einstellungen achte bitte wieder darauf, dass du eine Optionen fürs sichere Löschen angehakt hast. Z.b.: Sicheres Löschen - Komplexes Überschreiben (7 Durchgänge).

Die Einstellungen der Cookies überlassen wir dir, diesbezüglich ist es kaum möglich, eine allgemeingültige Empfehlung abzubilden, dazu spielen in dieser Hinsicht zu viele verschiedene Faktoren eine Rolle. Wenn du aber der Meinung bist, das deine besuchten Weltnetzseiten keinerlei individuelle Surfgewohnheiten speichern sollten, kann die Konsequenz nur lauten: keine Ausnahmen in die Cookie Liste eintragen.

Willst du neben den standardmäßigen temporären Ordnern noch weitere bereinigen, so ist das über die Rubrik Benutzerdefiniert möglich. Eine Liste für mögliche temporäre Ordner (nicht alle sind auch zwangsweise vorhanden) unter Windows haben wir für kurz skizziert:

Windows XP:

C:/Windows(slash)Temp
C:/Dokumente und Einstellungen/Administrator/Lokale Einstellungen/Temp
C:/Dokumente und Einstellungen/Default User/Lokale Einstellungen/Temp
C:/Dokumente und Einstellungen(/DeinBenutzername/Lokale Einstellungen/Temp

Windows Vista/ Windows7:

C:/Windows/Temp
C:/Benutzer/DeinBenutzername/AppData/Local/emp
C:/Benutzer/Default/AppData/Local/Temp

Erfahrungsgemäß sammelt sich in den etwas versteckten Ordnern nur sehr wenig an, insofern sind die cCleaner Voreinstellungen normalerweise ausreichend. Wer es trotzdem ausprobieren möchte, kann die entsprechenden Temp-Ordner als benutzerdefinierte Ordner im cCleaner eintragen.

Bleiben noch zwei Einstellungs-Rubriken übrig, einmal die Option Auschließen, wo du Ordner ausschließen kannst, die nicht in die Bereinigung einfließen sollen. Unter Erweitert sind noch ein paar grundsätzliche Einstellungen möglich, die du aber nicht verändern musst.
Registry-Cleaner:

Wie versprochen greifen wir an dieser Stelle das leidige Thema Registry-Cleaner noch einmal auf. Es ist wahrlich erschreckend, wie arglos einige Anwender diese Tools einsetzen, obwohl sie deren Wirkung weder verifizieren noch sicher einschätzen können. Besonders ärgerlich wird es, wenn einige Windows Foren sich zwar gegen die Verwendung dererlei Tools aussprechen, im Gegenzug aber Adsense Werbung mit eben diesen Tools ins Forum stellen, das ist wirklich „konsequent“.

Um es auf den Punkt zu bringen, es existiert kein kausaler geschweige denn evidenzbasierter Beweis, das Registry Cleaner irgend etwas positives bewirken. Wenn ein solches Tool nach der Neuinstallation von Windows bei einer Analyse 700 zu optimierende Einträge findet, in der Masse sind das dann hauptsächlich Verweise auf nicht mehr vorhandene Dateien ¿ nicht mehr vorhandene Verknüpfungen und nicht mehr vorhandene Programme, sollten wirklich alle Alarmglocken klingeln, weil das entbehrt nun wirklich jeglicher Logik.

In diesem Zusammenahng von „Tuning“ zu sprechen ist ohnehin der blanke Hohn, aber es hält sich seit Jahren der Mythos, die Registry muss regelmäßig mit Hilfsprogrammen entschlackt werden, damit Windows optimal arbeitet. Dies ist de facto falsch, die Registry ist eine Datenbank, in der Windows und viele Programme entsprechende Konfigurationsdaten speichern.

Dort werden auch keinerlei ini-Dateien abgearbeitet sondern Datenbanken abgefragt, d.h. installierte Programme und Applikationen fragen ihre Keys und Einstellungen diesbezüglich bei Bedarf in den entsprechenden Hives ab. Das bedeutet im Klartext, dass nach einer Deinstallation des jeweiligen Programms diese Datenbankinformationen eben nicht mehr abgefragt werden, ergo haben sie auch keinen Einfluss mehr aufs System, ob sie nun da sind oder nicht.

Ebenso falsch ist die Behauptung, das die komplette Registry Datenbank permanent in den Arbeitsspeicher geladen wird und somit wertvollen Speicherplatz belegt und Windows so verlangsamt. Es wird definitiv nur das in den Speicher geladen, was verwendet wird: also die benötigten Hives, alles andere bleibt draußen, demzufolge kann die Registry niemals Windows verlangsamen. Ganz davon abgesehn, dass ein einziger übereifriger Löschvorgang in der Registry ausreicht, um eurer Betriebssstem entscheidend zu kompromittieren. Wenn dein Windows zu langsam ist, rüste deine Hardware auf, die Registry ist diesbezüglich der komplett falsche Ansprechpartner...

8.60 WLAN Router - So schützt du dein Funknetz

WLAN (Wireless Local Area Network, zu Deutsch: WLAN, drahtloses, lokales Netzwerk) galt noch vor wenigen Jahren als Thema für Technikspezialisten. Das hat sich geändert. Immer mehr Menschen schätzen die Vorteile des mobilen Internets. Ob in Cafes, im Hotel oder zuhause:
Ein WLAN-Router - genügt, um sich mit seinem Computer oder Laptop ins Internet einzubuchen.

Hier kannst du dich Informieren wie du dein WLAN-Router und dein Funknetz einrichtest und verschlüsselst.

WLAN, Router, Hotspot: Was ist das?

Ein WLAN ist nichts anderes als ein lokales Funknetz. Im Mittelpunkt steht dabei der so genannte Access-Point (AP), Hotspot oder Router, der mit dem Internet verbunden ist. Mit einem passenden Gerät kannst du dich in diesen Hotspot oder Access Point per Funk einbuchen - und bekommst somit Zugang zum Internet. Die Reichweite der Funkverbindung hängt dabei von der eingesetzten Technik ab. In Gebäuden beträgt die Reichweite meist nicht mehr als 100 Meter. Im Freien und mit speziellen Antennen können durchaus mehrere Kilometer zwischen Access Point und Endgerät liegen. Der Standard, der WLAN möglich machte, wurde 1997 entwickelt.

Im Privathaushalt ist es in der Regel ein Router, der als Zugriffspunkt, dient. Dieser Router ist direkt mit dem Internet verbunden und sorgt über das Funknetz für die Anbindung der verschiedenen angeschlossenen Computer, etwa Laptops.

Gefahren bei WLAN
WLAN-Schutz: Richtig einrichten

Tarnkappen Router per Tor Netzwerk

Auf den folgenden Seiten zeigen wir wie du mit Hilfe des Tor-Netzwerkes deine Fritz!Box zu einem Tarnkappen-Router machst.

8.61 Gefahren bei WLAN

WLAN, sofern es ungesichert ist, lässt sich mit einer offenen Haustür vergleichen. Jeder, der in der Reichweite des Funknetzes ist, kann dieses mit entsprechender technischer Ausrüstung - einem so genannten Sniffer - aufspüren und sich Zugang zu deinem kabellosen Funknetz verschaffen. Und du als Betreiber des WLAN musst das nicht einmal merken.

Die Folgen:
Zum einen könnten Unbefugte auf deine Kosten ins Internet gehen. Und noch schlimmer: Außenstehende könnten - ohne dass du es bemerkst auf deine persönlichen Daten zugreifen. Ob Urlaubsfotos, Zugang und Passworte zum Konto oder deine höchstpersönlichen Daten: Alles könnte der Unbekannte aus sicherer Entfernung sichten, herunterladen und dann gegen dich verwenden.

Letztlich, auch das ist schon vorgekommen, kannst du unter Umständen sogar für kriminelle Aktivitäten Dritter in Haftung genommen werden. Stelle dir vor, ein Außenstehender surft auf deine Kosten über dein WLAN, und ersteigert mit deinen persönlichen Daten bei einem Internetauktionshaus kostspielige Waren. Oder er lädt sich illegal Musikstücke (mp3) oder Filme herunter. Oder: Ein Krimineller, gar ein Terrorist, nutzt dein WLAN, um sich mit Komplizen auszutauschen. Als Beispiel seien hier die islamistischen Terroristen genannt, die im Sommer 2007 in Deutschland mehrere Bombenanschläge verüben wollten. **Auch sie kommunizierten über das Internet - indem sie sich in ungesicherte WLAN-Netze Dritter einbuchten und so kaum identifizierbar ihrer kriminellen Aktivitäten nachgingen.**

Spätestens in solchen Fällen hast du ein großes Problem - nur, weil du dein Wireless LAN nicht ausreichend abgesichert hast. Denn Polizei, Anwälte und Abmahner haben in diesen Fällen zunächst einmal nur eins: Die IP-Adresse des Täters. Und das ist, wenn Dritte über deinen Internetzugang kriminell wurden, DEINE IP-Adresse, bzw. die deines Routers. Abmahnung, Hausdurchsuchung oder Ermittlungsverfahren werden also zunächst einmal gegen dich gerichtet sein.

Urteile: WLAN muss abgesichert werden

Auch die deutschen Gerichte urteilen immer öfter, dass jeder WLAN-Besitzer sein Funknetz gegen unbefugte Zugriffe schützen muss, weil er sonst zum so genannten Mitstörer wird. „Es ist einem Anschlussinhaber aber zuzumuten, zumindest Standardmaßnahmen zur Verschlüsselung des Netzwerks zu ergreifen; ansonsten verschafft er nämlich objektiv Dritten die Möglichkeit, sich hinter seiner Person zu verstecken und im Schutz der von ihm geschaffenen Anonymität ohne Angst vor Entdeckung ungestraft Urheberrechtsverletzungen zu begehen (...)“

stellte so das Landgericht Düsseldorf fest (Urteil vom 16.07.2008 - Az. 12 O 195/08).

Im Mai 2010 entschied dann auch der Bundesgerichtshof (BGH), dass private WLAN-Betreiber ihr Funknetz vor unberechtigten Zugriffen Dritter sichern müssen - durch eine angemessene Verschlüsselung und ein sicheres Passwort. Geschieht dies nicht, kann der WLAN-Betreiber im Fall von Urheberrechtsverletzungen Dritter abgemahnt werden und muss die entsprechenden Kosten zahlen.

8.62 WLAN-Schutz: Richtig einrichten

Dass sich viele WLAN-Besitzer in Gefahr begeben, liegt oft genug allein an reiner Bequemlichkeit. Man belässt es nach dem Kauf eines Systems einfach bei den Standardeinstellungen, die der Hersteller des WLAN vorgegeben hat - und vergisst dabei, dass diese Einstellungen eher auf Bedienungsfreundlichkeit, als auf Sicherheit ausgerichtet sind. Dabei lassen sich die Risiken mit wenigen Handgriffen und Einstellungen am Router und an den Endgeräten deutlich verringern:

Ändere an deinem Router die eingetragene SSID (SSID = Service Set Identifier) und die Kennwörter für deine Netzwerkgeräte. Diese werden nämlich von den Herstellern mit Standard-SSID und -Kennwörtern ausgeliefert. Sie sind damit natürlich auf allen ausgelieferten Geräten gleich, und damit auch Hackern bekannt. Als SSID sollte immer eine schwer zu erratende Kombination von Ziffern und Buchstaben gewählt werden. Wer seine SSID in „Heim-Netzwerk“ und „Stefan Müller“ umtauft, kann die Änderung gleich bleiben lassen - eine willkürliche Kombination nach Art von „8BrLk45awe“ ist weitaus sicherer. Um sich die Kombination zu merken, kann eine Eselsbrücke gute Dienste leisten.
Beachte hierzu auch das Kapitel: Das Passwort.
Beschränke die MAC-Adressen. Erlaube nur deinen eigenen Rechnern Zugriff auf den Access Point. Das lässt sich über die so genannten MAC-Adressen (MAC = Media Access Control) festlegen. Dafür trägst du die MAC-Adresse jedes von deinen verwendeten Computern oder Notebooks in den Access Point (Router) ein. Diese Adresse ist in der Netzwerkkarte gespeichert. Du ermittelst die Nummer mit dem Befehlszeilen-Tool Ipconfig.EXE (Start -¿ Ausführen -¿ CMD -¿ Ipconfig). Wenn du die Adressen eingetragen hast, und ein fremder Computer versucht, sich in dein Funknetz einzubuchen, wird er wegen der nicht übereinstimmenden Adresse abgewiesen.

Verschlüssel deine Kommunikation. Wenn du den Zugriff auf dein Netzwerk nur auf bestimmte MAC-Adressen beschränkst, und eine deinem lokalen Funknetz eine schwer zu erratende SSID gegeben hast, bist du auf dem Weg zu mehr Sicherheit schon einen guten Schritt weiter. Dennoch

ist der eigentliche Datenverkehr zwischen deinem Router und den Endgeräten noch völlig unverschlüsselt und kann abgefangen werden. Aktuell ist der Algorithmus WPA 2. Dieser verringert die Geschwindigkeit deines Funknetzes zwar ein wenig, doch dafür kann niemand mehr mitlesen, was du im Internet tust.
Schalte die Fernkonfiguration (Remote Management) ab. Fernkonfiguration ist eine feine Sache, wenn man sie braucht. Doch auch Unbefugte können dieses RRemote Managementffür ihre Zwecke nutzen. Wenn du diese Funktion nicht benötigst, deaktiviere sie.

Überprüfe Reichweite und Standort des Access Points (also des Routers).
Beim ersten Start deines Funk-Netzwerks solltest du unbedingt die Reichweite und den Standort deines Access Points überprüfen. Gehe dazu mit deinem Notebook oder Organizer ruhig aus dem Haus, stelle fest, in welcher Entfernung du noch auf das Netzwerk zugreifen kannst.

Spätestens dann solltest du bedenken:
So weit du von deinem Access Point entfernt sein kannst, so weit könnte auch ein Unbefugter entfernt sein - und sich trotzdem noch in dein Netzwerk einbuchen. Begrenze also die Reichweite deines Netzwerks so weit als möglich. Gegebenenfalls stelle den Access Point in der Wohnungsmitte auf.

Aktiviere das WLAN nur bei Bedarf und keinesfalls dauerhaft. Bei praktisch allen moderneren Routern ist das De-/Aktivieren des WLAN einfach per Tastendruck möglich; diese Taster sind allerdings - etwa bei der Fritz!Box wie auch beim Speedport W700/701/900V - relativ gut versteckt. Beim Speedport (700, 701, 900, nicht aber bei den Vorgängern 500/501) ist der entsprechende Taster auf der Rückseite des Geräts zu finden. Bei den ersten Fritz!Boxen ist dazu stattdessen ein kurzer Telefoncode möglich. Bei älteren Routern ist das De-/Aktivieren nur über den (Um-)Weg des Routerkonfigurationsmenüs möglich.

Wenn du alle oben aufgeführten Schritte befolgst, hast du schon ein gutes Stück zu deiner Sicherheit im kabellosen Netzwerk geschaffen. Zugleich solltest du dich weiter auf dem Laufenden halten. Überprüfe regelmäßig, ob für dein Netzwerk neue Sicherheits-Updates vorliegen. Informiere dich, ob neue Sicherheits-Lücken aufgetaucht sind, und wie du dich, deine Privatsphäre, deine Daten und dein Geld schützen kannst.

8.63 Tor-Proxy - Deine Fritz!Box als Tarnkappen-Router

Mit der Fritz!Box-Erweiterung Freetz bringst du deine Fritz!Box in den Stealth-Modus. Die Tor-Erweiterung erlaubt es bei Bedarf den gesamten ausgehenden Weltnetzverkehr über das anonyme Tor-Netzwerk zu leiten. Das Tor-Netzwerk leitet alle Anfragen - von Weltnetzseiten-Aufrufen und Suchanfragen bis hin zu Downloads - über drei verschiedene Server weltweit und versteckt damit deine IP-Adresse.

Der Clou: Das Tor-Plugin leistet das alles direkt im Router: Jeder Computer und jedes Smartphone können somit mit wenigen Handgriffen anonym im Weltnetz surfen.
Wer eine modifizierte Firmware mit seiner Fritz!Box verwendet, verliert die Gewährleistung des Herstellers. Im Test mit Freetz traten bei uns zwar keine Probleme auf, es kann aber vorkommen, dass etwa nach dem Flashen der Firmware die Fritz!Box nicht mehr erreichbar ist.

8.64 Freeware Freetz: So kommt Tor in die Fritz!Box

Damit Tor auf der Fritz!Box stabil läuft, sind einige Vorbereitungen nötig. Wir zeigen dir welche Software und Infos du vorab brauchst.

Das Prinzip von Freetz ist einfach: Du nimmst die Original-Firmware der Fritz!Box und mixt sie mit den Erweiterungen von Freetz zu einer eigenen Firmware. Für den Eigenbau der Fritz!Box-Firmware brauchst du eine Linux-Umgebung, die du am bequemsten in VirtualBox laufen lässt. Freetz versteht sich zwar auch mit Ubuntu oder Mint. Wir empfehlen aber Freetz-Linux.

Installiere also erst VirtualBox und werfe Freetz-Linux per Doppelklick an. Das Linux-System wird dann automatisch nach einem Klick auf „Importieren" als virtuelle Maschine in VirtualBox geladen.

Die virtuelle Maschine ist für eine Netzwerk-Bridge vorkonfiguriert. Diese musst du vorab in der Netzwerkumgebung von Windows einrichten.
Fritz!Box sichern

Achtung, das Experimentieren mit Fritz!Box-Firmware-Dateien sorgt nicht nur dafür, dass die Gewährleistung durch den Hersteller unwirksam wird, es kann deine Fritz!Box bei Fehlschlägen auch schrotten. Wir empfehlen deshalb zuerst ein Backup der aktuellen Fritz!Box-Einstellungen. Das klappt über die Fritz!Box-Oberfläche sowie über „System" und „Einstellungen sichern". Notiere dir außerdem noch einmal deine DSL-Zugangsdaten.

Tritt der Fritz!Box-GAU ein, solltest du auch einplanen, dass du offline bist und dir keine Rettungswerkzeuge mehr aus dem Weltnetz holen kannst. Deshalb solltest du dir vorab vom Fritz!Box-Server ein Recovery-Image für deine Box holen. Wichtig auch: Halte ein LAN-Kabel bereit, denn die Fritz!Box ist im Notfall meist nicht per WLAN erreichbar. Vorab solltest du dir auch diese Anleitung sichern, die beschreibt, wie man die Fritz!Box wiederbelebt.
Details zur Fritz!Box ermitteln

Für Freetz musst du das genaue Fritz!Box-Modell ermitteln, das verrät die Box in der Übersicht der Weboberfläche. Für Troubleshooting kann es auch wichtig sein zu wissen, wie viel Arbeits- und Flashspeicher die Fritz!Box besitzt. Hier hilft ein Blick unter www.fritz.box/html/support.html weiter. Klicke auf „Support-Daten erstellen". Die Fritz!Box erstellt dann eine Textdatei mit den wichtigsten Infos. Die gesuchten Werte findest du in den Zeilen „flashsize" und „memsize". Dabei bedeutet „flashsize=010000000" übersetzt 16 MByte Flashspeicher.

8.65 Fritz!Box-Firmware konfigurieren

Jetzt geht es ans Eingemachte. Du kannst dir eine angepasste Fritz!Box-Firmware nach deinem Geschmack bauen.

Starte Freetz-Linux in VirtualBox. Damit du mit dem System arbeiten kannst, musst du Benutzername und Passwort eingeben. Verwende dafür jeweils „freetz". Keine Bange, Fritz-Linux bringt keine grafische Oberfläche mit und die brauchst du auch gar nicht. Du landest stattdessen einfach in einer Kommandozeilen-Umgebung.

Der Befehl „svn checkout http://svn.freetz.org/branches/freetz-stable-2.0" holt das aktuelle Freetz-Paket. Ist es fertig geladen, siehst du nach eintippen des Befehls „ls" ein neues Verzeichnis. Per „cd freeze-2.0-stable" wechselst du in das neue Verzeichnis und kannst mit der Konfiguration starten.
Firmware konfigurieren

Über das Kommando „make menuconfig" startest du das Konfigurationsprogramm von Freetz.

Unter „Hardware type" musst du das genaue Fritz!Box-Modell auswählen. Wichtig auch: Unter „Firmware language" sollte „deutsch" eingestellt sein. Unter dem Menüpunkt „Packages" musst du zu „Standard Packages" wechseln und dort „Tor" auswählen. An dieser Stelle siehst du schon,

dass Freetz viele weitere Funktionen beherrscht, um eine Fritz!Box zu pimpen. Wenn es aber nur um Tor geht, bist du schon fertig. Verlasse nun das Konfigurationsprogramm via „Exit“ und wähle im nächsten Schritt „Yes“ um die Konfiguration zu speichern. Firmware erstellen

Über den Befehl „make“ wird deine ausgewählte Konfiguration jetzt in eine echte Firmware gegossen. Abhängig von der Geschwindigkeit deines Computers kann das auch schon mal 20 Minuten dauern. Leider gibt es keine Fortschrittsanzeige. Doch keine Panik, die durchlaufenden Meldungen musst du nicht verstehen. Wichtig ist, dass zum Schluss eine Erfolgsmeldung gezeigt wird und das Image fertig ist.

8.66 Firmware flashen und Tor einrichten

Die neue Firmware muss jetzt auf die Fritz!Box gepackt werden, danach kannst du mit der Tor-Konfiguration weitermachen.

Der Make-Befehl spuckt ein Fritz!Box-Image aus, das du im Unterverzeichnis „images“ findest. Dieses Image musst du jetzt über die Fritz-Weboberfläche einspielen. Eine Hürde ist jetzt, dass du das Image nur in der Konsole von Freetz-Linux im Zugriff hast und von dort aus nicht ohne Weiteres das Web-Interface der Fritz!Box erreichst. Die Macher von Freetz schlagen zwei Wege vor, wie man das Image von Linux auf Windows transportiert. Wir bevorzugen den Weg über WinSCP. Dazu musst du in Freetz-Linux über den Befehl „ifconfig“ die aktuelle IP-Adresse ermitteln und diese als „Rechnername“ in WinSCP eingeben.

Dann noch unter Benutzername und Kennwort jeweils „freetz“ eingeben und schon lässt sich eine Verbindung aufbauen.
Firmware flashen

Bis jetzt war alles Vorgeplänkel, bisher hast du deiner Fritz!Box noch kein Haar gekrümmt. Das ändert sich, wenn du unter „Einstellungen/System“ den Punkt „Firmware Update“ auswählst. Dort lädst du das neu erstellte Freetz-Image hoch. Ignoriere dabei den Warnhinweis, dass es sich um kein AVM-Original handelt.

Nach einem Neustart der Fritz!Box solltest du dich wie gewohnt an der Oberfläche anmelden können. Im Menü der Fritzbox findest du jetzt einen neuen Eintrag „Freetz“. Alternativ greifst du auch direkt via Port 81, also mit http://fritz.box:81 auf die Freetz-Oberfläche zu. Für den Login verwendest du den Benutzernamen „admin“ mit Passwort „freetz“.
Tor einrichten

Über ein grafisches Konfigurationsmenü kannst du Tor auf deine Bedürfnisse einstellen. Du kriegst als Voreinstellung einen kompilierten Tor-Proxy. Dieser läuft als reiner Client und ist dein Einstieg ins Tor-Netzwerk. Durch weitere Konfiguraitonsschritte ist es möglich, auch einen Tor-Server einzurichten, doch das ist erstmal nicht nötig.

Wichtig ist, dass du jetzt noch deinen Netzbetrachter als Proxy die Fritz!Box einstellst. Dann surfst du via Tor-Proxy. Ein möglicher nächster Schritt zur weiteren Absicherung wäre die Installation von Privoxy, auch dafür gibt es ein Modul in Freetz, das du beim Punkt „make menuconfig“ aktivieren kannst.

8.67 Tipps für mehr Geschwindigkeit

Tor ist für alle Nutzer gedacht, die ihre Privatsphäre im Weltnetz schützen wollen. Mit den richtigen Einstelllungen holst du mehr aus dem Proxy heraus.

Wenn es etwas gibt, das an Tor stört, dann ist es die Geschwindigkeit. Tor verschlüsselt den Datentraffic und schleust ihn dann auch noch zufällig über drei Server. Selbst mit einem Tor-Proxy dauern alltägliche Weltnetz-Aktivitäten damit spürbar länger.

Verwende Tor nicht für jede Aktion im Weltnetz. Spielst du Videos auf YouTube ab oder holst dir den Wetterbericht? Hier kann man Tor auch links liegen lassen. Schalte Tor dagegen für eBriefe, Chats, bei Weltnetz-Recherchen oder in Netzwerken und Foren gezielt ein.

Add-Ons für Tor
Einige kleine Helferlein erleichtern es dir, Tor in der Praxis in den Griff zu kriegen. So gibt es für Firefox beispielsweise den Torbutton, mit dem du das Tor-Netzwerk per Mausklick an- und abschalten kannst. Gebe dazu einfach in den Einstellungen von Torbutton als HTTP- und SSL-Proxy die IP-Adresse deiner Fritz!Box an. Dann wechselt Firefox automatisch auf den eingerichteten Tor-Proxy von Freetz. Wer oft zwischen Tor-Proxy und direktem Web-Zugang wechseln muss, sollte sich auch FoxyProxy genauer ansehen.

Geschwindigkeits-Optimierungen vornehmen
Eine Geschwindigkeits-Schraube an der man drehen kann, sind die verwendeten Tor-Server. Klar, der Einstieg ins Tor-Netzwerk erfolgt über den eigenen Proxy auf der Fritz!Box, aber wie geht es dann weiter. Tut man hier nichts, wird man zufällig einer Server-Kaskade zugeteilt. In der Freetz-Konfiguration kann man aber auch gezielt Eingangs- und Ausgangs-Server angeben. Passende Listen mit Servern gibt es etwa auf dieser Weltnetzseite.
Um zu prüfen, ob Tor funktioniert, sollte man Torcheck oder www.ip.s-f-n.org besuchen.

8.68 Weltnetz

Datenspuren beim „Surfen“

Wer Facebook oder andere Dienste nutzt (siehe Punkt: Soziale Netzwerke), bei denen ein Login nötig ist und dort unverschlüsselte Daten austauscht, erlaubt und ermöglicht jeden Kontakt, Seitenabruf, Chat und Klick eindeutig personenbezogen zu speichern und auszuwerten.

Bei Recherchen im Weltnetz können nicht nur Lauscher an Leitungen oder staatliche Lauscher an zentralen Knoten, das selbe Netzwerk oder WLAN nutzende Personen sowie dein Internetanbieter sehr leicht beobachten und speichern, welche Weltnetzseiten du abrufst. Anbieter der Weltnetzseiten können in den Logdateien des Webservers nachlesen, welche IP-Adresse wann welche Seiten abgerufen hat und über welche Links du gekommen bist. Selbst dynamische, also nur temporär vergebene IP-Adressen können spätestens vom Telekommunikationsanbieter und damit von Behörden dem jeweiligen Anschlussinhaber zugeordnet werden. Bei sensiblen Recherchen sollte deshalb die IP-Adresse verschleiert werden.

Zusätzlich zur erörterten Problematik der IP-Adressen gibt beim Aufruf von Links der sogenannte Referrer den Seitenbetreibern des verlinkten Angebotes Auskunft darüber, von welcher Weltnetzseite du kommst. Kommst du über eine Suchmaschine, ist dabei durch den Referrer für Seitenbetreiber auch nachvollziehbar, welche Suchanfragen du dort gestellt hast.

Desweiteren speichern Datenkraken wie z.B. Google nicht nur jeden Suchvorgang, Abruf und Klick, sondern verfolgen und speichern jeden mit technischen Tricks ausgeforschten Seitenabruf auch außerhalb der eigenen Dienste.

Um dich dabei dauerhaft verfolgen und eindeutig identifizieren zu können, vergeben solche Schnüffler dazu u.a. eine deine zugeordnete Nummer, die im Hintergrund in einem sogenannten Cookie auf

deinem Computer gespeichert und bei jedem der weiteren Abrufe wieder an die Schnüffler übertragen wird und diesen damit auch unabhängig von der unter Umständen wechselnden IP-Adresse mitzuteilen, wer was abruft und damit, welches Profil weiter gepflegt werden soll. So können über Jahre hinweg alle Suchen und Seitenabrufe diesen eindeutigen Nummern zugeordnet werden. Diese Nummern können wiederum - z.B. durch im Laufe der Zeit erfolgte Logins, anhand bestimmter IP-Adressen, den Spuren auf deinem Computer oder bestimmter Suchen oder Verhaltensmuster - mit dir in Verbindung gebracht werden.

Schützt du dich nicht gegen solches Tracking, erleichterst du das Anlegen und den potenziellen Missbrauch von sehr umfangreichen Profilen zu deiner Person, Arbeit und/oder Institution. (siehe Punkt: Tracking verhindern)

8.69 Anonymität im Weltnetz

Weshalb verschlüsselt und anonym surfen?

Wenn dein Internetverkehr unverschlüsselt und ohne Verschleierung der dir zuordenbaren IP-Adresse abläuft, hat das unter Umständen folgende Nachteile:

zum einen können Lauscher an der Leitung, das selbe Netzwerk oder WLAN nutzende Personen sowie dein Internetanbieter sehr leicht beobachten und speichern, welche Internetseiten du abrufst.

zum anderen können Anbieter der Weltnetzseiten sowie deren technische Dienstleister wie z.B. Google-Analytics unter anderem durch deine eindeutige IP-Adresse deine Identität herausfinden und damit ein Personenprofil über dich erstellen.

Deshalb bietet sich die Verschlüsselung wie auch die Anonymisierung der Seitenabrufe über das Anonymisierungsnetzwerk Tor an, über welches zudem auch technische Zensurmaßnahmen überwunden werden können.

Dabei werden deine Seitenabrufe nicht direkt und im Klartext mit deiner IP-Adresse zum Anbieter geschickt, sondern verschlüsselt über mehrere weltweit verteilte Rechner geleitet.

Erst der letzte Rechner in der Kette, der sogenannte Exit-Node, ruft dann die gewünschte Seite ab.

Dies geschieht ab diesem Zeitpunkt zwar meist auch unverschlüsselt, jedoch mit der IP-Adresse des Exit-Nodes sowie wegen den davorgeschalteten Knoten, die jeweils auch nur den vorherigen und nachfolgenden Knoten kennen, mit unbekanntem Empfänger.

8.70 Anonym surfen - Einleitung

Anonym surfen - das wünschen sich in Zeiten staatlicher Überwachung und gewerblicher Datenhändler viele Weltnetznutzer. Aber Anonymität im Weltnetz zu wahren ist komplizierter als man denkt. Sobald du deinen Computer mit dem Weltnetz verbindest, bist du identifizierbar. Von privaten und kommerziellen Datensammlern - aber auch von staatlichen Stellen. Anfang 2008 trat die Vorratsdatenspeicherung in Kraft. Seitdem wurde sechs Monate lang gespeichert, wann du mit wem telefonierst und wann du wo und wem eine SMS gesendet hast. Seit 2009 wurde nun auch ein halbes Jahr lang gespeichert, wann du wo und wie das Weltnetz genutzt hast. Im März kippte das Bundesverfassungsgericht die Massen-Speicherung zwar - allerdings nur vorerst. Eine „neue“, dann verfassungskonforme Vorratsdatenspeicherung ist schon in Vorbereitung.

Wenn du dich im Weltnetz anonym - oder zumindest weitgehend anonym - bewegen möchtest, musst du wissen, welche Spuren du dabei hinterlässt. Erst dann kannst du dich daran machen, deine Schritte zu verschleiern. Wir zeigen dir, wie es geht.

Beginnen wir mit der Frage, welche Spuren du im Weltnetz hinterlässt, und wie du dadurch identifiziert werden kannst.

-Diese Spuren hinterlässt du beim „Surfen“ durchs Weltnetz

Spur 1 im Weltnetz: die IP-Adresse

Du tippst einen Seitennamen in deinen Netzbetrachter ein und sofort erscheint die Seite? Kein Wunder, denn genau dafür gibt es die IP-Adresse. Jeder Computer im weltweiten Netz hat eine solche Adresse, quasi eine einzigartige Hausnummer. Das muss auch so sein, denn das Weltnetz ist nichts anderes als ein Verbund von Millionen Rechnern. Wenn in diesem Netz Informationen verschickt werden, benötigen diese eine „Anschrift“, wohin sie gehen sollen - eben die IP-Adresse deines Computers.

Mit dieser Adresse, die zum jeweiligen Zeitpunkt kein anderer Weltnetznutzer in der ganzen Welt hat, bist du problemlos - zum Beispiel von Ermittlungsbehörden - identifizierbar. Genauso einfach lässt sich dann auch herausfinden, über welchen Host du surfst, also wie der Server des Internetanbieters heißt, über den du gerade im Weltnetz bist.

IP-Adressen sind nach einem ganz bestimmten Schema aufgebaut. Sie bestehen grundsätzlich aus vier Dezimalzahlen, die mit Punkten getrennt sind. Damit kann es rein rechnerisch 4,3 Milliarden verschiedene Adressen dieser Art geben.

Bleibt die Frage, warum du keine Zahlenkolonnen eingeben musst, wenn du eine bestimmte Weltnetzseite besuchen willst. Des Rätsels Lösung sind so genannte Domain Name Server (DNS). Diese ordnen die Zahlenkolonnen den festen IP-Adressen (wie sie zum Beispiel Webseiten haben) zu. DNS arbeiten quasi als Übersetzer - und erleichtern so das Surfen im Weltnetz enorm.

Feste IP-Adresse, dynamische IP-Adresse
Die Zahl der IP-Adressen im Weltnetz ist begrenzt. Deshalb haben Provider wie etwa T-Online einen großen Pool solcher Adressen. Wenn du ins Weltnetz gehst, weist dir dein Provider eine gerade freie IP-Adresse aus diesem Pool für den Zeitraum deiner Sitzung zu. Das nennt man eine dynamische IP-Adresse.

Etwas anderes liegt der Fall, wenn du selbst einen Server betreibst oder über eine größere Firma ins Weltnetz gehst. Diese verfügen häufig über eine feste IP-Adresse.

Jedes Mal, wenn du während deiner Weltnetzsitzung aktiv wirst, ob du nun eine Seite besuchst, Dateien auf deinen Rechner herunterlädst, Filme ansiehst oder Musik anhörst, wird deine IP-Adresse unsichtbar an dein „Gegenüber“ versendet, also an den Rechner, mit dem dein Computer gerade kommuniziert. So weiß dieser, wohin er seine Daten schicken muss, damit sie auch ankommen.

Schon die IP-Adresse, die dir zugeteilt ist, verrät eine Menge über dich. So lässt sich recht genau zurückverfolgen, an welchem Punkt in der Welt du dich eingewählt hast. Gehst du nun über eine feste IP-Adresse ins Netz, etwa über ein Firmennetzwerk, lässt sich dein Standpunkt durch eine Rückverfolgung (den so genannten Traceroute) auf wenige Meter genau feststellen. Bei einer dynamischen IP-Adresse wird das schon schwieriger. Endgültig identifizierbar wirst du dann allerdings in Verbindung mit deinen Verbindungsdaten.

Spur 2 im Weltnetz: Deine Verbindungsdaten
Wenn du dich ins Weltnetz einwählst, speichert dein Diensteanbieter die Verbindungsdaten von dir. Dazu gehört die IP-Adresse, die dir zugewiesen wurde, Beginn und Ende der Verbindung mit Datum und Uhrzeit, und, sofern dies zur Abrechnung nötig ist, die Menge der übertragenen Daten. Im Rahmen der Vorratsspeicherung werden deine Verbindungsdaten sechs Monate lang bei den Diensteanbietern gespeichert um sie im Falle von Ermittlungen den Behörden zur Verfügung stellen zu können.
Spur 3 im Weltnetz: Bestandsdaten
Um im Weltnetz surfen zu können, benötigst du - wie schon oben dargestellt - einen Anbieter, der dir den Zugang zum Web zur Verfügung stellt. Egal, ob du diesen Zugang nun über Modem, ISDN oder DSL herstellst, musst du dich bei deinem „Internet Service Provider“ (ISP) anmelden. Die dafür nötigen Daten heißen Bestandsdaten und werden natürlich auch gespeichert.

Zu den Bestandsdaten gehören Namen und Anschrift, Rechnungsadresse und weitere Kontaktdaten (Telefon, Fax, eBriefadresse). Diese Daten müssen, so will es das Telemediengesetz (TMG), „für Zwecke der Strafverfolgung, zur Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes oder des Militärischen Abschirmdienstes“ von Diensteanbietern herausgegeben werden.

Spur 4 im Weltnetz: Server-Protokolle
Nicht nur dein „Internet Service Provider“ zeichnet auf, wann du mit welcher IP-Adresse online bist. Auch dein jeweiliger „Gegenüber“ protokolliert deine Besuche mit. Wenn du eine Weltnetzseite besuchst, greifst du auf einen Server zu, also einen Rechner, auf dem die jeweiligen Seiten (oder von dir abgerufenen Dokumente, Filme, Bilder etc.) liegen. Diese Zugriffe werden automatisch in Logfiles (Protokollen) aufgezeichnet.

Zu den gespeicherten Daten zählen unter anderem die IP-Adresse des Besuchers, der Zeitpunkt, in vielen Fällen auch Daten wie das Herkunftsland des Besuchers, sein Betriebssystem, die Sprache seines Netzbetrachters und vieles andere wie beispielsweise der Referrer. Darunter versteht man die Weltnetzseite, von der du gerade gekommen bist. Was mit all diesen Daten geschieht, kannst du als Besucher nicht wissen.

8.71 Das Ende der Anonymität im Weltnetz?

Die Kombination von IP-Adresse und Speicherung von Bestands- und Verbindungsdaten ist - zumindest für den Erhalt von Anonymität und Privatsphäre im Weltnetz - verhängnisvoll. Dein Diensteanbieter speichert deinen Namen und deine Adresse, er zeichnet auf, wann und wie du ins Weltnetz gehst, samt deiner jeweiligen individuellen IP-Adresse. Gleichzeitig teilst du beim Surfen der „anderen Seite“ ständig mit, welche IP-Adresse du hast, und kannst so relativ genau lokalisiert werden. Und auch diese Daten werden gespeichert - wobei du keinen Einfluss darauf hast, wie sie letztlich genutzt werden.

Wir haben gesehen, dass du im Weltnetz verschiedene Spuren hinterlässt. Diese können nun zusammengeführt werden und so zu deiner Identifizierung verwendet werden. Diese Zusammenführung ist auf verschiedene Weise möglich:

- Ermittlungsbehörden: Die Kombination von IP-Adresse und Verbindungsdaten ist für eine gewisse Zeit bei deinem Diensteanbieter gespeichert. In dieser Zeit können Ermittlungsbehörden die Daten abfragen und damit überprüfen, ob du womöglich eine Straftat im Weltnetz begangen hast. Die Vorratsdatenspeicherung läuft seit Januar 2009 in Deutschland. Damit werden die Verbindungsdaten sechs Monate lang gespeichert.
- Private Dritte: Private Dritte, zum Beispiel auch Unternehmen aus der Film- und Musikindustrie, können über einen Umweg an Daten kommen, um dich zu identifizieren. Sie

müssen einfach nur Strafanzeige bei einer Staatsanwaltschaft gegen Unbekannt erstatten. Wenn die Fahnder dann ermitteln und beim Provider deine Identität ermitteln, müssen die Unternehmen nur noch über ihren Anwalt um Akteneinsicht bitten - schon sind deine höchstpersönlichen Daten und deine Identität bekannt.

- Musik Film und Softwareindustrie: Im Rahmen der EU-Gesetzgebung hat die deutsche Bundesregierung auch einen zivilrechtlichen Auskunftsanspruch gegenüber Providern eingeführt. Das betrifft vor allem das Tauschen illegal kopierter Musik, Software und Filme im Weltnetz (Filesharing). In diesem Fall können Firmen zur Durchsetzung von Schadensersatzforderungen einfach bei den Internetprovidern die Verkehrsdaten von Verdächtigen abfragen - ohne Umweg über die Staatsanwaltschaft. Damit bist du also auch von privaten Dritten relativ einfach identifizierbar.

IP-Adresse und Identität im Weltnetz verschleiern

Auf den nächsten Seiten zeigen wir dir, wie du deine verräterische IP-Adresse so verschleiern kannst, so dass anonymes Surfen zumindest bedingt möglich wird:

8.72 Sicherheit durch UMTS-Sticks

Wer sich diesen ganzen VPN-Proxy-Krims-Krams sparen will, sich aber donnoch sicher im Weltnetz bewegen möchte kann sich einen anonymen UMTS-Stick und eine anonyme Sim-Karte kaufen. Die WLAN Verbindung an deinem Computer ausgeschaltet geht man nur über den anonymen UMTS Zugang ins Weltnetz.

So erreichst du mit wenig Aufwand ein hohes Maß an Anonymität, da viele Nutzer gleichzeitig über diese vom Zugangsanbieter generierten IP-Adresse ins Weltnetz gelangen. Der Zugangsanbieter, dessen Mobilfunknetz du nutzt, ist nach wie vor in der Lage, anhand der SIM-Karte und Seriennummer des USB-Sticks (International Mobile Equipment Identity, kurz IMEI) zu identifizieren. Dazu aber später mehr ...

UMTS Stick kaufen
Natürlich kaufst du den Stick in Bar und nicht im Weltnetz. Du kannst dir bei Aldi, Lidl oder einem ähnlichen Discounter einen unlocked UMTS-Stick kaufen. Dieser kostet um die 39.99 Euro und ist von der Geschwindigkeit meist noch nicht mal schlecht. Einfach eine anonyme Simkarte egal welchen Anbieters da rein und schon kann es losgehen.

Anonyme Sim-Karte
Die Besorgung der anonymen Sim-Karte verläuft ähnlich. Man geht leicht vermummt in einen Laden und kauft eine Sim-Karte. Diese kann man dann telefonisch (am besten mit einem Wegwerftelefon) oder aus einem „Internet-Cafe“ aktivieren[1].

Aldi Talk (12 Euro Startguthaben, 15 Euro Monatsflat, 2 Euro Tagesflat, teure Pro-MB-Abrechnung)
Congstar (10 Euro Startguthaben, 10 Euro Monatsflat, teure Minutenabrechnung)

Preislich sind Aldi Talk und Congstar recht gut. Du kannst aber aus vielen weiteren Sim-Karten Anbietern wählen. Eine Flatrate lohnt sich da natürlich, vor allem, wenn man wirklich viel macht.

Surfen mit dem UMTS-Stick
Die Installation der Sticks ist auch einfach gehalten, die meisten installieren sich von selbst quasi „Plug & Play“. Es ist schlau, nicht nur von zuhause den Stick zu benutzen, da die Funkzellen,

[1] Dieses Vorgehen hat der Gesetzgeber in der BRD unterbunden. Unter Umst änden ist dies im Ausland noch möglich.

Zugangszeitpunkt, dauer der Verbindung, Datenvolumen pro Verbindung, IMEI und Mobilfunknummer beim verbinden und surfen gespeichert werden. Wenn du dich nur von Zuhause ins Weltnetz einwählst kann man recht simpel deinen Standort zuordnen.

Allgemeines zur Sicherheit mit UMTS-Sticks
Selbst mit UMTS-Stick ist man natürlich nie ganz sicher. Was nützt der anonyme UMTS-Stick ohne das man ihn in einen Comuter oder Laptop einsteckt. Ein Laptop, den man überall einsetzen kann ist natürlich optimal. UMTS-Sticks verbinden sich über das Mobilfunknetz mit dem Weltnetz. Dadurch sind sie auf 10 m genau ortbar, zumindest laut einigen

Quellen im Weltnetz
Du solltest dir immer eine neue Sim-Karte kaufen und diese nicht wieder aufladen. Das Startguthaben ist eh immer genau so hoch wie der Preis bzw. in manchen Fällen sogar noch höher. Aufladen lohnt sich also nicht.

Wir empfehlen dir den UMTS-Stick auch alle 4 Sim-Karten mal zu wechseln und einen neuen kaufen. Dabei geht es nicht nur um die Ortbarkeit, sondern auch darum, dass im Falle von Ermittlungen euch natürlich bereits durchgegangene Aktionen mittels der IMEI-Nummer angehangen werden können. Daher ständig Stick und Sim-Karte wechseln.

8.73 VPN Server

Ein Virtual Private Network (VPN) ist ein Computernetz, welches zum Transport privater Daten ein öffentliches Netz, zum Beispiel das Weltnetz, nutzt. Die Verbindung über das öffentliche Netz wird üblicherweise verchlüsselt. Es ermöglicht somit eine sichere Übertragung über ein unsicheres Netzwerk. Teilnehmer eines VPN können Daten wie in einem LAN (lokales Netzwerk) austauschen. Die einzelnen Teilnehmer selbst müssen hierzu nicht direkt miteinander verbunden sein. Eine Verbindung der Netze wird über einen Tunnel zwischen VPN-Client, dem Benutzer Zuhause, und dem VPN-Server ermöglicht. Meist wird der Tunnel dabei gesichtert, aber auch ein ungesicherter Klartexttunnel ist ein VPN.

Der VPN-Client ist eine Software, die eine verschlüsselte und authentifizierte Verbindung zum VPN-Server aufbaut.

Folgende Punkte sind bei der Benützung von VPN wichtig:

- Der Computer, auf welchem die VPN-Verbindung aufgebaut wird, sollte mit einem aktuellen Antivirusprogramm ausgestattet sein, das sich täglich updated.
- Der VPN-Client sollte nur aktiviert sein, wenn lizenzierte Weltnetzseiten besucht werden.
- Die VPN-Software darf nicht an dritte weitergegeben werden.

Leider können nach der Installation von VPN Schwierigkeiten auftreten, wie beispielsweise, dass sich der Computer verlangsamt. Weiter verunmöglichen einige Firewalls, nicht die von Windows, ein Aufbauen der Verbindung, was nur mit einer Deinstallation des Programms umgangen werden kann.
Wenn du, wie von uns Empfohlen, die Personal Firewall von Comodo benutzt findest du in diesem Leitfaden die passenden Einstellungen um den VPN-Verkehr richtig durch die Firewall zu leiten.

8.74 Methoden zur Verschlüsselung und Anonymisierung

Es gibt viele Möglichkeiten, seine Spuren im Weltnetz zu verschlüsseln. Dabei unterscheidet man generell zwischen zwei Methoden, der Verschlüsselung und der Tunnelung (von engl. tunneling, natürlich kein richtiges deutsches Wort). Was das bedeutet, lässt sich recht einfach am Beispiel eines Briefes verdeutlichen.

Wenn du einen Brief verschickst und nicht willst, dass der Brief auf dich zurückzuführen ist, so gibt es zwei Möglichkeiten. Du gibst den Brief einer Person, die den Inhalt verschlüsselt und erst dann versendet oder du gibst den Brief einer Person, die ihn in deinem Namen versendet und dich so anonymisiert. Natürlich gilt dies auch für „Briefe“, die du empfängst, nur umgekehrt.

Später werden wir sehen, dass es am besten ist, die Briefe auf beide Arten zu anonymisieren und am allerbesten auch noch durch zwei verschiedene Personen.

Gut, dann stellen wir dir mal diese beiden Personen vor, sie heißen VPN und Sock5

VPN (der Verschlüsseler)
VPN steht für Virtual Private Network. Der Name sagt eigentlich schon alles. Man verbindet mit seinem Computer, also mit seiner IP, zu einem Server. Dieser Server bindet den Computer dann in das „Heimnetzwerk“ ein, sodass die Daten zuerst an den Server gesendet werden und dann an den eigenen Computer, also ein virtuelles Heimnetzwerk. VPN-Server haben verschiedene Funktionen, uns interessiert in unserem Falle aber nur die Funktion der Verschlüsselung.

Das VPN verwendet Login-Daten, damit nur berechtige (hier: zahlende) Nutzer Zugriff auf den Server haben und zusätzlich werden die eingehenden und ausgehenden Daten egal welcher Art sicher und „unknackbar“ verschlüsselt. So kann keiner deinen Traffic abfangen und die Daten auslesen, da sie verschlüsselt sind. Die Analogie zu der Person, die einem den oben erwähnten Brief verschlüsselt und dann versendet, wird nun klar.

SSH-Tunnel und Sock5
Möchte man seine IP verschlüsseln (ggf. nachdem man den Traffic-Inhalt bereits per VPN verschlüsselt hat), dann verwendet man so genannte SSH-Tunnel und Sock5-Server. Das Sock5-Protokoll ermöglicht mittels Authentifizierung (mit den Login-Daten des Anonymisierungs-Anbieters, den man verwendet) das Tunneln der Daten, was am Ende dazu führt, dass man „nach außen hin“ nicht mehr seine eigene IP hat, sondern die IP des Socks-Proxys.

SSH-Tunnel (auch SSH-Socks genannt) verschlüsseln zusätzlich die Daten mittels SSH (Secure Shell). Der Sock-Server ist also die Person, die deinen Brief nach der Person, die ihn verschlüsselt hat, erhält und diesen in seinem Namen an den Empfänger schickt, der SSH-Tunnel verschlüsselt den Brief dann noch zusätzlich.

Dabei richtet man zuerst den SSH-Tunnel ein und anschließend den Sock5.

vicSock
Da man zur Erhöhung der Sicherheit einen Sock-Server auswählt, der juristisch am besten „weit weg“ ist (z.B. China, Russland, Afrika), hat man natürlich dadurch die IP des Serverstandorts. Mittels IP-Geotagging können Seiten (wie welche, die ihr z.B. besuchen wollt) so euren Standort ermitteln und euch den Zugriff, egal welcher Art, verwehren. Eine afrikanische IP bestellt für gewöhnlich nicht bei Amazon nach Köln.

Deswegen schaltet man noch hinter den Sock5-Proxy einen vicSock. Dieser führt dazu, dass du eine deutsche IP hast. vicSocks werden erstellt, in dem man Schadsoftware auf einen Computer bringt, der es dann ermöglicht, eben diesen, wenn er im Weltnetz ist, als Proxy zu verwenden.

Man erhält dann die IP des Schadsoftware-Victims, daher auch der Name vicSock.

Da das Implementieren von Schadsoftware mittels ePost, BOTs oder Ähnlichem natürlich nicht legal ist, kannst du keine vicSocks bei renommierten Anonymisierungsdienstleistern erwerben, sondern musst diese auf Szene-Seiten (www.vic-socks.to)coder bei Vendorn in Untergrund-Szene-Foren kaufen. Manchmal findet man auch welche in der Free-Section von Untergrund-Szene-Foren, die funktionieren. Hat man erst mal einen vicSock, der nicht auf der Blacklist ist (auch unique vicSock genannt), kann man den Seiten, auf denen man surft, vortäuschen, man hätte eine normale deutsche IP und das, obwohl man einen VPN-Server und einen Sock5-Server verwendet, die weit weg von Deutschland stehen.

Wichtig ist hierbei, dass es sich um einen Non-Logging vicSock handelt, einen, der die IP also nicht loggt. Dabei musst du natürlich auf den Szene-Service, den du für die vicSocks nutzt, oder eben den Vendor, bei dem du die vicSocks kaufst, vertrauen.

Grundlegendes
Manche Leute schwören darauf, einen VPN-Server, danach einen SSH-Tunnel und dahinter zwei oder sogar mehr Sock5-Server zu schalten (und dann ggf. den vicSock). Das ist an sich nicht empfehlenswert, da alle Server bei einem Anbieter sind. Die Anzahl der hintereinander geschalteten Server von einem Anbieter erhöht nicht die Sicherheit, da es sich trotzdem nur um einen einzigen Briefwechsel zwischen Ermittlungsbehörde und Anbieter handelt, wenn dieser deine Daten rausgibt, dann macht er das auch, wenn du 10 Sock5-Server hintereinander geschaltet hast.

Daher empfiehlt es sich, Anbieter zu kombinieren.

So kann man z.B. VPN (Perfect Privacy) + SSH Tunnel (Perfect Privacy) + Sock5 (Socks Service) verwenden. Sollte Perfect Privacy loggen und IPs rausgeben, so schützt dich immer noch Socks Service und umgekehrt. Das ist eigentlich die einzige Methode, die Sicherheit erneut zu steigern.

Nachdem man nun die grundlegenden Begriffe verinnerlicht hat, muss man sich für einen bzw. lt. Tipp für mindestens zwei Anbieter entscheiden.

8.75 VPN Anbieter

Das wichtigste Werbemittel aller VPN Anbieter ist das nicht vorhandene Logging der IPs. Genutzt wird das Angebot von wohl allen Spektren aus der Gesellschaft - und zwar weltweit. Wer im Weltnetz was macht, interessiert Perfrct Privacy nicht die Bohne. Mehr Informationen über den VPN Provider Perfect Privacy findest du in unserem Infoblog: www.blog.s-f-n.org/tag/perfect-privacy

Weiterhin solltet ihr euch die Informationen über das sog. IP-Logging im Infoblog durchlesen.
www.blog.s-f-n.org/tag/ip-logging
Dass solche Dinge gerade europäischen Zensurbehörden ein Dorn im Auge sind, ist ganz klar. Schließlich wird seit Jahren ein System durchgesetzt, in dem der Bürger allgegenwärtiger Überwachung unterliegt und sich dadurch scheuen soll, seine Meinung frei zu äußern und sich frei zu verhalten.
www.perfect-privacy.com
Meiner Meinung nach einer der besten Anonymisierungs-Anbieter. Die Server sind verhältnismäßig schnell, die Standorte sind recht gut gewählt und der Support ist wirklich super, hinzu kommt noch ein nicht allzu hoher Preis.

Angebot: VPN, PPTP VPN, SSH-Tunnel, Sock5
Monatsgebühr: 25 Euro
Mengenrabatt?: Ja

2 Jahresgebühr: 350 Euro, sprich 10,50 Euro pro Monat
Zahlungsmittel: PayPal, Amex, Mastercard, Visa, eCheck, PaySafeCard und WebMoney.
Serverstandorte: Australien, China (Hong Kong, Shanghai), Malaysia, Israel, Rumänien, Tschechien, Schweden, Russland, Ukraine; Deutschland, Schweiz, Luxemburg, Niederlande, Frankreich, Vereintes Königreich, Kanada, USA, Panama und Argentinien
Vorteile: Große Serveranzahl, gute Geschwindigkeit, guter Support, verhältnismäßig günstig, PP bietet seinen Kunden einen bereits vorkonfigurierten SSH-Client an, nur noch Server auswählen, Login-Daten eintragen und fertig.
Nachteile: Viele Server stehen in Ländern, die es mit dem Datenschutz nicht so ernst nehmen (z.B. USA), diese sollte man daher lieber nicht verwenden - am Ende bleiben dann doch nur ca. 7 Server, die verwendet werden sollten.

Die Registrierung verläuft mit PaySafeCard ziemlich anonym, daher würde ich grundsätzlich diese Bezahlmethode verwenden.

Ist dir Perfect Privacy zu Teuer oder traust du diesem Dienst nicht, kannst du in dieser VPN Provider Übersicht weitere Dienste finden.

8.76 Einrichten der Anonymisierung

Hier werden wir Schritt für Schritt und gut bebildert die Anonymisierung vom Schritt der Registrierung bei einem Anonymisierungsdienst bis hin zum endgültigen Check bei einem IP-Checker erklären. Dabei können wir natürlich nicht auf alle Anonymisierungsdienste eingehen, da wir aber immer Perfect Privacy empfehlen, zeigen wir dir die Einrichtung mit den Perfect Privacy Diensten.

Im Prinzip ist es jedoch überall gleich und man kann die hier aufgeführten Informationen analog auf alle anderen Dienstleister anwenden.

8.77 Zahlungsmittel besorgen, Registrieren und Bezahlen

Nachdem du dich entschieden hast, welchen VPN Anbieter du verwenden möchtest gehst du zu einer Tankstelle, ziehst dir im Sommer eine Sonnenbrille und im Winter einen Mütze mit dickem Schal an und kaufst dort den Paysafecard-Wert, den man für die Registrierung benötigt. Du kannst auf www.Paysafecard.com nachschauen wo es in deiner Umgebung die Karten zu kaufen gibt.

Wenn du nun den Paysafecard-Code gekauft hast gehst du auf www.perfect-privacy.com und wählst unter Perfect Privacy VPN Prices dass Paket das du Buchen möchtest.

Im nächsten Abschnitt gibst du einen Benutzernamen, eine ePost-Adresse, dein Betriebssystem an. Danach wählst du die sichere Zahlmethode: Paysavecard. Es kann immer mal vorkommen das z.B. beim Serverstandort Deutschland, eine Perfect-Privacy Festplatte oder gar ein ganzer Server von der Polizei beschlagnahmt wird. In diesem Fall kann die Polizei auf der Festplatte des Servers deinen Benutzernamen sehen. Deswegen ist es extrem wichtig einen Benutzernamen zu wählen mit dem du im Weltnetz und auch im normalem Leben nichts zu tun hast und auch kein 2. mal verwendest. Das gleiche gilt als sicherheitsmaßnahme auch für die ePost-Adresse.

Haken rein bei „I read the Terms and Conditions“, ...ünd mit einem Klick auf Submit bestätigst du den Kauf.

Nun heisst es erstmal abwarten. Es meldet sich „ein Admin“ per eBrief bei dir und fragt nach dem Paysafecard Code. Diesen schickst du ihm zu und bekommst innerhalb von höchstens 48 Stunden die Login-Daten für den Mitgliederbereich und natürlich auch die Server. Meistens geht es aber

schneller.

Nachdem du die Zugangsdaten erhalten hast, kannst du dich in den Mitgliederbereich von Perfect-Privacy anmelden und erhälst dort alle notwendigen Informationen, sprich Server IPs, spezielle Programme (wie vorkonfiguriere SSH-Clienten) und ziemlich gut beschriebene Tutorials zum Einrichten.

Leider sind diese oft auf Englisch, weshalb wir hier noch mal alles haargenau und mit Bildern erklären (siehe Netzseite unter www.s-f-n.org).

8.78 Nach Erhalt der Zugangsdaten einrichten des VPN

Nachdem du die Zugangsdaten zum Mitgliederbereich erhalten hast, kannst du dich nun an das Einrichten der Anonymisierung machen. Dazu muss Open VPN heruntergeladen werden. Dabei handelt es sich um ein Open Source VPN-Client, der demnach auch kostenlos ist.

Nachdem du den Clienten runtergeladen hast, installierst du diesen, startest ihn aber noch nicht **(Bilder unter www.s-f-n.org)**.

Open VPN lässt sich recht einfach konfigurieren, da alle Anonymisierungs-Anbieter die Konfigurationsdateien für Open VPN zum Download anbieten. Diese müssen dann nur noch in den richtigen Ordner kopiert werden und Open VPN ist dann bereits richtig konfiguriert, dann brauchst du nur noch den VPN-Server auswählen, mit dem du dich verbinden willst, und bist mit diesem verbunden, nachdem du die Zugangsdaten eingegeben hast.

Du loggst dich bei Perfect Privacy (oder bei einem anderen Anbieter) ein und lädst im Download Bereich die Config-Dateien für Open VPN runter. Dazu gehst du bei Perfect Privacy in den Download-Bereich und lädst unter „OpenVPN Config Files“ die Open VPN-Konfigurationsdateien für alle Server runter, dann kannst du später bei openVPN einfach einen der vielen Server auswählen.

Dabei erhältst du eine zip-Datei. Diese extrahierst du mit dem Windows-eigenen Entpacker, Winzip oder Winrar. Im Ordner, in den du die Zip-Datei extrahiert hast, finden sich nun viele Dateien, hier mal ein Bild.

Diese Dateien musst du nun in den Config-Ordner von Open VPN kopieren. Dieser befindet sich standardmäßig, in Windows XP unter: C:/Programme/OpenVPN/config und ab Windows Vista im Ordner: c:/Program Files/OpenVPN/config - das kann natürlich bei dir auch anders sein, dann kopierst du die Dateien halt in den config-Ordner an dem Ort, wo du Open VPN hin installiert hast.

Jetzt kannst du endlich die Open VPN GUI starten, also die auf Windows abgestimmte Benutzeroberfläche von Open VPN. Dabei ist wirklich sehr, sehr wichtig, dass du das Programm als Administrator startest. Mit Rechtsklick auf Eigenschaften geklickt, lässt sich das Programm immer als Adminstrator starten, dazu nur einen Haken bei „Programm als Adminstrator ausführen“, im eigenschaftenmenü unter dem Reiter Kompatibilität setzen. Wenn du das Programm nicht als Adminstrator startest, dann funktioniert es nicht richtig und deine richtige IP wird trotzdem vermittelt.

Ein kleines Icon entsteht im System Tray (zwei nebeneinander stehende Monitore). Die Monitore leuchten rot, wenn keine Verbindung besteht, gelb, wenn eine Verbindung aufgebaut wird und Grün, wenn eine Verbindung zu einem VPN Server besteht.

Klickt man mit der rechten Maustaste auf das Icon von Open VPN, so kann man, wenn man die Konfigurationsdateien richtig in den config-Ordner kopiert hat, einen Server auswählen, auf den

connectet werden soll.

Für welchen Server man sich entscheidet, sollte an sich klar sein. Man nimmt natürlich keine europäischen Server, sondern lieber Ostasiatische oder Afrikanische.

Wenn man nicht weiß, für welchen Server man sich zwecks besserer Geschwindigkeit entscheiden soll, dann gibts im Mitgliederbereich deines Anbieters eine Liste der Server mitsamt allen Informationen. Dort steht neben der Server-IP und den Ports auch die Auslastung des Servers.

Also Server auswählen und auf Connect klicken.

Es öffnet sich, nachdem man einen Server ausgewählt hat, ein Fenster und nach einigen Sekunden wird man nach den Login-Daten gefragt, die man dann einträgt.

Nach einigen Sekunden sollte eine Verbindung aufgebaut sein, indem sich dieses Fenster schließt.

Die Monitore im Tray-Icon leuchten grün und eine kleine Meldung erscheint, dass eine Verbindung zum Server hergestellt worden ist, z.B. HongKong.

Nachdem nun eine Verbindung mittels Open VPN hergestellt wurde, sind alle Daten des Ein- und Ausgangstraffics verschlüsselt. Überprüft man nun seine IP bei einem IP-Checker, dann erscheint die IP des VPN-Servers. Leider ist die DNS dann immer noch deutsch, dies ändern wir später.

Wie man sieht, ist die eigene IP und DNS nur mit Open VPN nicht ganz sicher, deswegen schaltet man einen Sock5-Server dahinter, ich verwende hier zuerst einen SSH-Tunnel und danach einen Sock5.

-Einrichten des SSH-Tunnel mittels Perfect Privacy SSH-Client

Der Vorteil bei Perfect Privacy liegt darin, dass der Dienstleister euch einen eigens vorkonfigurierten SSH-Clienten anbietet.

Im Mitgliederbereich von Perfect Privacy kannst du den Clienten unter Downloads runterladen. Danach installierst du diesen. Open VPN ist ja bereits gestartet und verbunden, dann kannst du natürlich auch hier wieder ganz wichtig:

Den Perfect Privacy SSH-Client mit Adminstratorrechten starten.
Du suchst dir einen Server aus (natürlich nicht den selben wie bei Open VPN), gibst die Zugangsdaten ein, machst einen Haken bei „Passwort speichern“ und bei „Dauerhafte Verbindung“. Die Haken bei „Automatische Verbindung“ und bei „SSH über HTTP Proxy“ lässt du weg.

Nun klickst du auf Verbinden. Nach einigen Sekunden verschwindet das Programm (bleibt aber natürlich im System Tray), die Verbindung ist hergestellt. Zusätzlich erscheint neben dem System-Tray Icon des Perfect Privacy SSH-Client ein kleines gelbes Logo, das bedeutet das du verbunden bist.

Um sicher zu gehen kannst du den Client aus dem System Tray heraus starten und kannst dort sehen, ob du verbunden bist. Wenn du alles richtig gemacht hast, dann sollte es so aussehen.

Also: VPN Monitore beide grün, SSH Client mit gelbem Icon.

-Einrichten des SSH-Tunnels mittels Putty bei anderen Anbietern als Perfect Privacy

Wenn du nicht Perfect Privacy verwendest, dann musst du einen anderen SSH Client verwenden. Das ist auch nicht viel komplizierter. Dazu verwenden wir das Freeware-Programm PuTTY. Dieses kannst du unter www.putty.org runterladen.

Installiere PuTTY und starte es mit Adminstratorrechten, das Programm muss nicht installiert werden.

Nun gibst du die IP des Servers auf dem Startbildschirm bzw. unter Session und dann Logging ein. Bei manchen Anbietern ist die IP des Servers eingetragen als eine domain, z.B. shanghai.perfect-privacy.com, hier trägst du natürlich den Servernamen ein. Als Port trägst du den vom Anbieter angegebenen SSH-Port für den Server auf den du verbinden willst an (meist: 22).

Jetzt musst du noch ein, zwei Einstellungen vornehmen, die ich aus Zeitgründen hier nicht weiter erläutern werde. Es gibt zahlreiche Tutorials zu PuTTY, die du ohne Probleme verwenden kannst. Die Einstellung ist ohnehin immer die gleiche. Zusätzlich findest du bei deinem Anonymisierungsdienstanbieter Tutorials zur Einrichtung des SSH-Tunnels mittels PuTTY.

8.79 Einrichten von Proxifier für den Sock5

Nun möchten wir hinter den VPN - SSH Tunnel - Verbund noch einen Sock5 schalten. Das ist eine weitere Sicherheitsmaßnahme, natürlich nur, wenn man wieder einen anderen Serverstandort wählt.

Proxifier ist ein Programm, was laufende Programme überwacht und, falls diese Daten aus dem Internet empfangen bzw. welche senden, diese Daten durch einen Proxy tunnelt. Der Vorteil bei Proxifier liegt darin, dass man nicht jedes Programm einzeln konfigurieren muss, sondern im Proxifier Regeln für jedes einzelne oder alle Programme konfigurieren kann und diese dann entsprechend der Regel getunnelt werden.

Zuerst musst du dir das Programm unter www.proxifier.com herunterladen.

Nach der installation von Proxifier startest du es wie Open VPN und den SSH-Clienten mit Administratorenrechten.

Proxifier startet (unter Umständen) minimiert im Systemtray als graues Viereck. Wenn du alles richtig konfiguriert hast, dann füllt sich dieses Viereck, wenn Daten gesendet bzw. empfangen werden. Das wirst du ja hoffentlich später sehen.

Im Proxifier gehst du oben auf Profile und wählst dann Proxy Servers aus.

Danach öffnet sich das Proxy Servers Menü.

Hier klickst du einfach oben rechts auf den Button „Add“. Dort gibst du unter Server Adress „localhost“ ein (natürlich ohne Anfürhungszeichen) und als Port 8050. Wichtig: Der Port ist unter Umständen bei anderen Anbietern anders. Das ist aber nicht kompliziert und man versteht das recht einfach.

Um nun die Daten von Proxifier durch den SSH-Sock-Server schicken zu lassen, muss Proxifier natürlich den internen Port vom Localhost-Sock-Server haben (local port).

Dieser ist bei Perfect Privacy 8050.

Jetzt machst du einen Haken bei „Socks Version 5“ und noch einen Haken bei „Authentification“, dann kannst du deine Zugangsdaten, die du vom VPN Betreiber bekommen hast, eintragen. Zuletzt mit „OK“ den Server in die Proxifier-Serverliste aufnehmen. Also alles wie auf dem Bild.

Du kannst mittels Druck auf den Button „Check“ die Verbindung überprüfen. Wenn du viel grüne Schrift siehst, ist alles ok, ansonsten hast du irgendwie einen Fehler gemacht. Nachdem du auf „OK“ geklickt hast, fragt dich Proxifier, ob du den localhost-Server als Standard-Proxy nehmen willst, was du bejahst.

Der Localhost-Server erscheint nun oben in der Server Liste, wie auf folgendem Bild.

Nun trägst du genau wie eben einen neuen Server ein (auf Add klicken) aber du trägst als Server IP nicht localhost ein, sondern die IP des Servers an, den du als Sock5 verwenden willst. Als Port trägst du hier den Externen Port (Remote Port) des Sock5-Servers ein. Ansonsten ist alles gleich wie beim localhost-Server.

Dies kannst du natürlich beliebig oft wiederholen und alle Server deines Anbieters eintragen. VicSocks bitte nur benutzen wenn du weißt was du machst!

Falls du einen vicSock verwenden möchtest, kannst du ihn genau so hinzu wie die Sock5-Server hinzufügen, nur dass du keine Authentifikation benötigst. Einfach die IP eintragen, den Port, Sock5 auswählen und ohne Authentifikation auf OK.

Nun müssen wir natürlich dafür sorgen, dass die Daten, die vom VPN Server zum SSH-Tunnel-Server gehen danach durch den Sock5-Server gehen. Wir empfehlen lieber einen Sock5-Server eines anderen Anbieters als zwei Sock5-Server hintereinander zuschalten, die beim gleichen Anbieter sind.

Um dies also zu bewerkstelligen, musst du eine Kette von Servern einstellen, also eine Proxy Chain. Die Daten werden dabei durch jeden der eingetragenen Proxies geroutet, und zwar in der Reihenfolge, wie sie in der Chain angeordnet sind.

Im gleichen Menü, in dem du per „Add“ Server hinzugefügt hast, kannst du im unteren Bereich über dem „Cancel Button“ auf „Proxy Chain“ gehen.

Danach erstellst du eine neue Proxy-Chain, indem du auf „Create“ klickst und benennst diese nach Belieben, zum Verständnis heißt sie bei uns „Chain 1“.

Unsere „Chain 1“ erscheint nun in der Proxy Chain-Liste und wird mit „Empty“, also leer, beschrieben.

Dies wollen wir natürlich ändern und die Chain füllen.

Nun markierst du den localhost-Server aus der Proxifier-Serverliste und zieht diese per Drag and Drop in die gerade erstellte Proxy Chain „Chain 1“.

Wenn du alles richtig gemacht hast, erscheint nun der Server localhost in der Proxy Chain und ein Haken ist davor gesetzt. Diesen Haken belässt du drin.

Auf die gleiche Art und Weise ziehst du nun den oder die Sock5-Server in die Chain „Chain 1“, die du verwenden willst. Du kannst auch einfach alle Server rüberziehen, da du in der Kette ohnehin durch Haken setzen oder entfernen entscheiden kannst, welche Server in der Chain verwendet werden und welche nicht. Wir ziehen hier nur einen Sock5-Server (Kairo) und einen vicSock rüber.

Nehmen wir an du hast einen Sock5, was ja wie gesagt, ausreicht und einen vicSock. Also, sind in der Server Chain nun drei Server; localhost, dein Sock5-Server und der vicSock.

Sehr wichtig ist, dass der Server localhost als erster in der Liste ist! Die Sock5-Server kommen danach, in unserem Fall nur einer (zumidnest bei nur einem ist ein Haken gesetzt, die ohne Haken sind ohnehin „ausgestellt“). Wenn du einen vicSock verwendest, dann fügst du natürlich noch diesen als letzten Server in die Chain und setzt einen Haken davor.

Wenn du alles richtig gemacht hast, sieht das Menü im Proxifier so aus:

Danach kannst du das Menü schließen.

Nachdem du nun eine Server-Chain erstellt hast, machst du dich daran, für die Programme, die du verwendest, einzustellen, dass diese durch eben jene gerade erstelle Server-Chain getunnelt werden. Um das einzustellen, gehst du im Proxifier oben auf Profile und klickst dann auf „Proxification Rules“.

Wenn sich das Proxification Rules-Menü öffnet, dann sind dort bereits zwei Regeln eingestellt. Eine heißt „localhost“ und eine „default“.

Bei Localhost kannst du bei „Action“ (herunterfahrbares Menü) „direct“ eingestellt lassen. Es geht dabei ohnehin nur um interne Netzwerkzugriffe und die brauchen wir nicht zu tunneln, also „direct“ einstellen.

Bei der Regel „default“ wählst du bei Action (herunterfahrbares Menü) „Chain Chain 1“ aus.

Wenn du alles richtig gemacht hast, dann sieht das aus wie auf dem Bild.

Jetzt musst du für die Programme Regeln erstellen. Dies kannst du entweder für alle Programme einstellen oder eben für ausgewählte, wie z.B. Firefox. Prinzipiell kann man alle Programme tunneln lassen.

Du gehst also unten links auf „Add“ und kannst dort eine Regel eintragen.

Name: trage hier den Namen des Programms ein
Applications: Gehe auf „Browse“ und dort zur .exe Datei des zu tunnelnden Programms. Z.B. auf „C:/Programme/Firefox“ und wähle dort die „firefox.exe“ aus.
Willst du alle Programme tunneln, so kannst du in das Feld das Wort „Any“ eintragen, natürlich ohne Anführungszeichen.
Target Hosts: Dieses Feld ist dafür gedacht um bestimmte IPs oder Domains auszuwählen. Dann wird das Programm nur dann getunnelt, wenn es diese IPs oder Domains anfragt. Hier trägst du einfach „Any“ ein, da alle Ziel-Adressen getunnelt werden sollen.
Target Ports: Du kannst auch nur bei bestimmten Ports tunneln lassen. In unserem Fall, wo alle Zieladressen und Ports getunnelt werden sollen, trägst du auch hier „Any“ ein.
Action: Hier kannst du auswählen, durch welchen Server bzw. welche Chain das Programm getunnelt wird. In unserem Fall wählen wir die gerade erstellte Chain „Chain 1“ aus.

Wenn du alles richtig eingestellt hast, sieht das Menü wie folgt aus:

Klicke nun auf OK.

Du hast nun entweder nur für Firefox bzw. für ein anderes Programm deiner Wahl oder eben für alle Programme („Any“ eingetragen bei Applications) das Tunneling eingestellt. Die Daten wandern vom VPN zum SSH und dann zum Sock5 und ggf. noch zum vicSoc und dann zu dir.

Besser gehts nicht ...

8.80 DNS an den Proxy anpassen

Ein Blick auf einen IP-Checker zeigt dir, dass immer noch deine deutsche DNS mitgesendet wird. Das ist zwar nicht ganz so schlimm wie das Mitsenden der IP aber immer noch zurück verfolgbar. Das wollen wir natürlich umgehen.

Man kann in den Netzwerkeinstellungen rumspielen, im Config-Menü (about:config) vom Firefox oder einfach Proxifier darauf einstellen.

Dazu einfach im Proxifier oben auf „Profile“ gehen und dann auf „Name Resolution“ klicken.

Im aufgegangenen Menü machst du nur einen Haken bei „Resolve hostname through Proxy“, die Haken bei „Detect DNS Settings automatically“ und „Try to resolve via local DNS Service first“ müssen draußen sein.

Wenn du alles richtig eingestellt hast, sieht das aus wie folgt.

Nun ist alles richtig eingestellt und du kannst deinen Erfolg bei einem IP-Checker überprüfen ... im Firefox selber musst du nichts mehr einstellen und auch in keinem anderen Programm, Proxifier übernimmt die Tunnelung durch die Proxies für alle Programme, die du ausgewählt hast.

8.81 Mac-Adresse bzw. IMEI (bei UMTS-Sticks)

Bei deiner Mac-Adresse brauchst du dir an sich keine Sorgen zu machen. Diese wird nicht über das Weltnetz übertragen. Wie das bei IMEI-Nummern bei UMTS-Sticks ist, können wir nicht genau sagen. Soweit wir wissen sendet man bei jedem Connect die IMEI-Nummer des Sticks an den Sim-Karten-Provider.

Wenn man mit einem Anonymen-UMTS-Stick und einer Anonymen-Simkarte im Weltnetz ist, braucht man auch keine Anonymisierungsdienste (VPN usw), sollte nur einiges beachten. Sicherheitsvorkehrungen bei UMTS-Sticks kannst du im Thema Sicherheit durch UMTS-Sticks nachlesen.

Die Mac-Adresse ist nur dann wichtig zu beachten, wenn du ein offenes W-Lan als Weltnetzquelle nutzt. Da der Router die Mac-Adresse aller verbundenen Computer (bzw. eher gesagt ihrer Netzwerkkarten) loggt, musst du da natürlich bevor du disconnectet in das Menü des Routers gehen und dort die Logs löschen. Wenn das Routermenü nicht passwortgesichert ist, sollte das kein Problem sein.

Im Falle von Anonymisierung durch VPN+SSH Sock+Sock5 ist kein Verschleiern oder Ändern der Mac-Adresse notwendig, da wir uns ja nicht in ein offenes W-Lan verbinden.

8.82 Der erste Test

Nun kannst du zum Beispiel Firefox starten. Wenn du alles richtig gemacht hast, erscheint Firefox nach dem Start im Proxifier Connections Menü und unten siehst du, wie die empfangenen und gesendeten Daten durch die Kette „Chain 1“ getunnelt werden, wenn du eine Adresse bei Firefox eingibst.

Das sieht dann so aus, wie auf dem Bild. Das graue Proxifier-Viereck im System Tray füllt sich zusätzlich noch Blau (Datentransfer).

Gehe nun auf die Seite **www.ip.s-f-n.org**. Wenn du alles richtig gemacht hast, siehst du dort die IP, den Standort und den DNS des Sock5-Servers.

Die Seite müsste bei dir so aussehen, dann hast du, wenn Proxifier augenscheinlich läuft, alles richtig gemacht. Natürlich kannst du auch auf jede, dir bekannte Seite gehen, z.B. www.wieistmeineip.de

Wie du siehst, ist Java bei mir Deaktiviert. Bei dir wird das wohl als aktiviert angezeigt. Das heißt du bist noch nicht fertig, also weiter gehs ...

-Zusätzliches zur Erhöhung der Anonymisierung (Wichtig, nicht leichtfertig behandeln)

Da nicht nur der Netzbetrachter oder das benutzte Programm deine IP oder andere Informationen versenden, sondern auch Programme, die im Hintergrund laufen, müssen diese deaktiviert werden.

Speziell sind da Java, Flash und Anti-Viren Programme gemeint. Grundsätzlich auch jede Software, die du legal erworben hast und die Rückschlüsse auf deine Lizenzinformationen zulässt. An sich ist es zwar ziemlich unwahrscheinlich, dass der Software-Hersteller überhaupt nach deinen Lizenzdaten gefragt wird, aber Sicherheit geht ja bekanntlich vor.

Flash:
Kannst du getrost ausschalten, einfach über Systemsteuerungen deaktivieren. Für die meisten Anwendungsgebiete ist Flash nicht unbedingt von Nöten. Es gibt nämlich so genannte LSOs oder Super Cookies, das sind Flash Cookies, die zu Sicherheitszwecken verwendet werden. Pay Pal verwendet diese zum Beispiel, so kann Pay Pal erkennen, dass es sich um die selbe Person handelt, wenn diese mit den selben Flash Cookies aber mit zwei Accounts einloggt.

Wenn du Flash nicht ausschalten willst, dann gibt es für den Firefox das Addon Better Privacy. Dieses ermöglicht dir, richtig eingestellt, dass Firefox automatisch alle Flash Cookies/LSOs/Super Cookies löscht, sobald er geschlossen wird.
Java:
Java solltest du auch deaktivieren. Benötigt wird es nicht und es sendet unter Umständen die richtige IP mit. Daher solltest du es wirklich deaktivieren, dies kannst du unter Systemsteuerungen machen.
Java-Script:
Java-Script stellt keine Gefahr da, kannst du getrost anlassen. Weitere Infos bekommst du auf der Seite: JavaScript / JScript Anti-Viren-Programme:
Diese kannst du, musst du aber nicht ausschalten. Die Antiviren-Programme könnten Rückschlüsse auf deine Lizenzinformationen und damit auf eure Rechnungsadresse zulassen. Bei kostenfreien Antiviren-Programmen wie wir es mit Avira AntiVir Personal Free empfohlen haben ist das natürlich kein Problem.
Welchen Netzbetrachter soll ich nehmen?
Die Frage lässt sich in meinen Augen recht leicht beantworten, Mozilla Firefox.
Kleiner Tipp, lade dir Portable Firefox herunter (http://portableapps.com/apps/internet/firefox_portable) und „installiere“ diesen. Dieser wird nicht direkt installiert, sondern startet komplett aus dem Ordner heraus, in das dieser entpackt wurde. So kannst du einen eigenen Firefox nur dafür verwenden, auf Seiten der Bewegung zu lesen. Was du mit diesem Firefox Portable macht beeinflusst deinen normalen Firefox Netzbetrachter nicht.
Wichtig: Nicht vergessen, dann natürlich auch eine Regel im Proxifier für den Portable Firefox zu erstellen, falls du nicht eh eine Regel „Any“ für alle Programme gemacht hast.

Die einfachste Methode:

Wenn du deinen Firefox Netzbetrachter oder den Portable-Firefox verwendest und keine Lust hast, Flash und Java einzeln abzustellen, dann kannst du dir mittels des Firefox Addon-Appstores das Add On Quick Java runterladen.

Ist es installiert, erscheint im Firefox unten rechts die Möglichkeit, Java, Java Script, Flash und Silverlight direkt auszuschalten. Beachte dann aber bitte, dass diese Funktionen nur im Firefox ausgeschaltet sind, daher ist es immer noch am besten, diese direkt zu deaktivieren (es sei denn du benutzt wirklich nur Firefox und sonst nichts).

So sieht das dann aus, sehr effektiv:

Du bist Fertig, deine IP ist verschlüsselt, deine Daten sind verschlüsselt, deine DNS ist verdeckt und Java und Flash stellen für dich keine Gefahr mehr da. Super!

Wie du auf dem Bild noch erkennen kannst, ist Google bei mir auf Arabisch. Wenn man nicht gerade „Deutsch“ als Sprache im Firefox, sondern „Automatisch“ ausgewählt hat, dann zeigt dir Google natürlich die Sprache an, aus dessen Land du für Google connectet, und das ist in meinem Fall Ägypten

8.83 DNS Leak

Wenn ein Anonymisierungs Dienst benutzt wird, ist es extrem wichtig das jeglicher Traffic der von deinem Computer geht durch das anonyme Netzwerk gerouted wird. Ist das nicht der Fall, ensteht ein sogenannter Leak, dein Netzwerkverkehr bzw. deine DNS Anfragen laufen nicht über das anonyme Netzwerk und somit kann trotzdem nachvollzogen werden welche Weltnetzseiten du besucht hast. Was ist ein DNS Leak?

Sobald eine Domain z.B. www.s-f-n.org aufgerufen wird, fragt der DNS-Server die zugehörige IP Adresse ab. Solltest du dich hinter einem Router befinden, dann wird der DNS-Server deines ISPs im Router gesetzt und dein Rechner stellt die DNS-Anfragen an deinen Router.

Allerdings kann es vorkommen, dass dein Betriebssystem, je nach Konfiguration, weiterhin die Anfragen an deinen Router richtet. Dadurch setzt du dich einem unnötigen Sicherheitsrisiko aus, denn sollte eine Seite die Anfrage deines DNS-Servers mitschneiden, dann ist es möglich, sofern dein DNS-Server ebenfalls Logs mitschneidet, deine echte IP-Adresse herauszufinden. Wie Teste ich, ob ich betroffen bin?

Verbinde dich zunächst mit dem VPN und rufe DNS leak test auf. Dort kannst du testen, ob du ebenfalls davon betroffen bist. Klicke auf „Check DNS leaks now!“. Wird bei dem Ergebnis eine IP-Adresse aus deinem Land und vor allem deines ISP ausgegeben, dann bist du betroffen.

Wie verhindere ich einen DNS Leak?
Um einen DNS Leak zu vermeiden bzw. zu verhindern gibt es mehrere Möglichkeiten. Die wohl einfachste ist es, einen public DNS Dienst anstelle des Provider-eigenen zu benutzen.

Hier eine kleine Auswahl an öffentlichen DNS Diensten:

Comodo public DNS

NS1: 156.154.70.22
NS2: 156.154.71.22

Google public DNS

NS1: 8.8.8.8
NS2: 8.8.4.4

OpenDNS public DNS

NS1: 208.67.222.222
NS2: 208.67.220.220

DNSAdvantadge public DNS

NS1: 156.154.70.1
NS2: 156.154.71.1

ChaosComputerClub

85.214.20.141
204.152.184.76 (f.6to4-servers.net, ISC, USA)
2001:4f8:0:2::14 (f.6to4-servers.net, IPv6, ISC)
194.150.168.168 (dns.as250.net; Berlin/Frankfurt)
213.73.91.35 (dnscache.berlin.ccc.de)

Wie du einen Alternativen DNS Dienst in deinem Netzbetrachter einstellen kannst haben wir im Thema Netzbetrachter beschrieben.

8.84 Die digitalen Wolken: Die Cloud Computing Falle?

Cloud Computing. Der neue Hype der digitalen Naivitätsmanie. Cool seien die Wolken, praktisch - und kostengünstig. Wer keinen Cloud hat, nicht alles im Cloud verwahrt - der ist altmodisch und dumm. Negativ eingestellt zur schönen neuen Welt sozusagen. Ein Eldorado für den Schnüffelstaat, ein Datenspeicher ohne Backupgarantie, ein Hackertummelfeld könnten Clouds nicht sein? So wird die gesamte Datenmasse von Firmen und das gesamte digitale Leben von Privatpersonen zur digitalen Wolke. Virtuell und unbeständig schwebt sie am Himmel - heute hier und morgen schon weg?

Die surreale Datenwolke. Daten, die einem nicht wirklich gehören, auf die man bei Verlust keinen Anspruch hat, bei Diebstahl keine Verteidigungsmöglichkeit. Die nun seit Jahren gehypte IT Revolution der Kostenersparnis und Bequemlichkeit, das ultimative Gadget des weltweiten Zugriffs, die zuckersüsse Welt der virtuellen Applikationen.

Die Wolke ist cool, kann schon sein, sie ist Milliardenbusiness, kann schon sein - aber ist sie vernünftig?

Gekünstelt sei die Aufregung um den NSA Abhörskandal, keiner Rede wert der neue Yottabyte Datenspeicher in Bluffdale, normale Terrorabwehrmassnahme das neue Deutsche 100 Millionen BND Schüffelprogramm. Denn wir würden sowieso schon überall und immerfort abgehört, dass wisse man schliesslich schon lange. Dabei ist es genau dieser Fatalismus, der uns immer mehr kapitulieren lässt vor Big Brother Total. Irgendwann hängen dann Kameras und Mikrophone bei uns zuhause, irgendwann gibt es dann wirklich kein zurück mehr und das Wort Privatsphäre wird entgültig aus dem Lexikon gestrichen. In nur ein paar Jahren werden uns dann unsere Kinder ungläubig anstarren, wenn wir das Wort Privatsphäre auch nur in den Mund nehmen und erstaunt fragen: „Papa, Mama - was ist das?“

Deshalb dieser Artikel zur Datenwolke. Das immens gehypte Cloud Computing soll Firmen flexibler und kostengünstiger ihre IT Bedürfnisse abwickeln lassen und versetzt auch progressive Privat-

anwender in euphorische Gadget Stimmung. So wurde der Author kürzlich schief angeschaut von einem Cloud Computing Fan - und nach leiser Kritik an der Wolkerei als nicht genug positiv eingestellter Mensch verrissen.

8.85 Sind Daten in einer Cloud sicher?

Apple Mitbegründer Wozniak meint lapidar, Cloud Computing sei des Ende des Eigentumsrechts.

In der heutigen digitalen Welt würde man laut dem Apple-Mitbegründer „kaum mehr etwas besitzen", weil alles in der Cloud gespeichert ist. Außerdem würde der Benutzer durch die verschiedenen Abos sämtliche Rechte abgeben. Wenn der Benutzer hier in Ungnade fällt, könnte laut Wozniak der Provider den Zugang verwehren und sämtliche Dateien wären weg. „Als ich aufwuchs, war der Unterschied zwischen Russland und den USA das Eigentumsrecht", gab der 62-Jährige an.

Und Matt Honan, ein erfahrener IT Author - Senior Journalist beim Amerikanischen Magazin Wired - berichtet, wie sein gesamtes digitales Leben im Verlauf einer Stunde zerstört wurde:

Innerhalb einer Stunde wurde mein gesamtes digitales Leben zerstört. Erst wurde Google-Konto übernommen, anschließend gelöscht. Weiter mein Twitter-Account kompromittiert und als Plattform für rassistische und homophobe Nachrichten benutzt. Und das Schlimmste von allem, man war mein AppleID Konto eingebrochen und mein Hacker benutzte es, um aus der Ferne alle Daten auf meinem iPhone, dem iPad und meinem MacBook zu löschen ... Apple-Tech-Support gab den Hackern die Möglichkeit, auf mein iCloud-Konto zuzugreifen. Amazon Tech Support gab ihnen die Möglichkeit, einen Teil der Informationen zu sehen - ein Teil der Kreditkartennummer ... um die Identitätsprüfung durchzuführen. Diese Unvereinbarkeit deckt Fehler in Daten Management Strategien, welche endemisch sind in der gesamten IT-Branche, auf und weist auf einen drohenden Alptraum hin, in den wie uns im Zeitalter des Cloud Computing und der vernetzten Geräten begeben

Ein Alptraum ist es wirklich. Und das zeigt sich schon an ein paar eBriefe, welche ich gestern erhalten hatte. Denn meine Tochter hatte meine eBrief Adresse für Ihren Facebook Account angegeben. Wohl mit einem einfachen Passwort, welches gehackt wurde. Der erste eBrief teilte mir mit, dass ein neues Passwort gesetzt wurde, der zweite, dass diese eBrief Adresse entfernt wurde. Und schon sind ihre Hunderten von Freundinnen einem Spammer oder Schlimmeres aus Casablana, Marokko ausgesetzt. Das sie jetzt nicht mehr auf Facebook kann, finde ich durchaus beruhigend, aber der Rest... und hier geht es nicht einmal um Cloud Computing. In 10 Minuten war meine Tochter nicht mehr meine Tochter auf Facebook - sondern das war jetzt einfach irgendwer anderes. Identity theft - stehlen der Identität, nennt sich das. Damit wird im besten Fall „nur" ein Facebook Konto kompromitiert - und im nur etwas ernsteren Fall eine ganze Existenz.

Das wirft die ernsthafte Frage auf: Wie naiv gehen wir eigentlich kollektiv mit unseren „eigenen" Daten um?

Und, wie immer, sind US Unternehmen auch im Cloud Computing global federführend. Sie haben die besten Angebote, sind die bekanntesten Anbieter.

- Rund 90 Prozent dieses Cloud Computing finden in den USA statt, wo der reichlich kurze Arm des deutschen Datenschutzes nichts auszurichten vermag und Ansichten, denen zufolge Privatsphäre eine Illusion ist, Beifall finden.

  Das heisst aber auch, dass 90% (oder sind es doch wohl eher 100% ?) der Cloud Daten dem NSA Überwachungsapparat ausgesetzt sind. Ahnungslos und scheinbar unendlich naiv geben Firmen so ihre zentralen Geheimnisse der Wolke preis - und Privatanwender ihre gesamten privaten Daten stolz in die wirre Datenwolke der digitalen Beliebigkeit.

- Wenn Cloud-Daten von der EU in die USA überführt werden, würden diese dem dortigen Überwachungsapparat ausgesetzt. Das müsse jedem Betroffenen mitgeteilt werden.

  So berichten inzwischen auch cloudfreundliche Publikationen, dass der neuste NSA Skandal Cloud Paranoiker in ihrer Ansicht bestärken werde, dass Clouds gefährlich sind.

- Während wir hin zu öffentlichen Wolken migrieren, sind die lautesten Kritiker dieser Entwicklung auch der Meinung, dass die Daten dadurch einer grösseren Gefahr ausgesetzt werden, durch Behörden überwacht zu werden. Während man ihnen Mechanismen und Statistiken zeigen kann, welche den Wert von öffentlichen Wolken zeigen, wird der NSA Oel im Feuer der bereits Wolke Paranoiden sein

  Aber wenn man den stolzen Cloud Anbietern - welche mit digitalen Superlativen nur so um sich werfen - nicht trauen kann, Daten vor dem NSA und anderen Behörden zu schützen, was macht es denn für einen Sinn, private bzw. firmeninterne Informationen in einem Cloud zu lagern?

- Es ist fraglos, dass in der Aera von Smartphones und Tablet Computing über mehrere Geräte hinweg die Option von Cloud Computing sehr atrraktiv ist ... Aber ich frage mich ob man Apple nicht vertrauen kann. Meine Informationen werden ohne Gerichtsbeschluss an Behörden weitergegeben, wieso sollte ich meine Informationen ihren Cloud Servern anvertrauen, sogar wenn sie verschlüsselt sind?

- Ich sollte es nicht tun - und du auch nicht.

  So sind Daten im Cloud weder ausreichend vor Geheimdienstspäherei, noch vor Hacking, noch vor Datenverlust geschützt. Man legt mit einem Cloud auch die Hohheit über die eigenen Daten ab, macht sie ultratransparent. Mit dem Vorteil, dass man auf diese von beliebiger Stelle her zugreifen kann. Gib dem (Cloud-)Teufel einen Finger, so nimmt er die die ganze Hand, könnte es heissen...

- Am Ende des Tages, wenn du überlebenswichtige Daten und Informationen in den Besitz von einem Drittanbieter gibst - Cloud oder auf andere weise - kann die Annahme das dein Anbieter seine Umgebungen vollständig kontrollieren kann bezweifelt werden.

  So kann sich ein Cloud Angreifer alle Zeit der Welt nehmen, um an die sensiblen Daten zu kommen, die Firmenidentidät oder die persönliche Identität zu stehlen, zu kompromitieren oder gar ganz auszulöschen.

  Ist Cloud Computing nicht einfach ein weiterer Hype der Industrie - zur grossen Freude der Geheimdienste, der Datendiebe, der Hacker? So äussert sich sogar der CEO des Datenbankgiganten Oracle abschätzig über den Ultrahype Cloud Computing.

- Die interessante Sache an Cloud Computing ist, dass wir Cloud Computing so definieren, dass es alles beinhaltet, was wir sowieso schon tun. Ich kann an nichts denken, dass nicht Cloud Computing ist, mit all diesen Ankündigungen. Die Computer-Industrie ist die einzige Branche, die mehr als Frauenmode getrieben ist.

  Und so ist es bei den Cloud Anbietern Programm und Teil der Allgemeinen Bedingungen, keine Sicherheit zu bieten. Kunden nutzen Cloud Computing auf eigene Gefahr. Wer haftet, wenn die Cloud alles vergisst? Allein der Kunde...

- Evernote schreibt, man garantiere nicht für die Sicherheit des Dienstes, Kunden würden ihn auf eigene Gefahr nutzen. So ähnlich formulieren es auch die Cloud-Anbieter GoogleDrive, iCloud und Dropbox.

  Wie soll die Sicherheit des Cloud Computings gewährleistet werden? Alles läuft über den Netzbetrachter, die Sicherheitsabfragen sind oft sehr primitiv, über Social Engineering - so Beispielsweise Anfragen beim technischen Dienst - ist ein Fremdzugang oft sehr einfach zu bewerkstelligen.

- Das große Thema eines Cloud basierenden Modells ist die Fähigkeit, weitgehend von überall aus einloggen zu können, und die Tatsache, dass es meistens über einen Netzbetrachter ausgeliefert wird. In den meisten Fällen sind die Anmeldeinformationen trivial. In den meisten Cloud-Umgebungen gibt es kein Konzept von Intrusion Abwehr oder Prävention.

  So erstaunt es nicht, dass neben Geheimdiensten auch Hacker und Kriminelle die Cloud entdeckt haben. So wurden beispielsweise bei Sony über Amazons Cloud 100 Millionen Kundendaten gehackt. Nur 100 Millionen - wie lächerlich ist denn das?

- Es sieht ganz danach aus, als hätten auch Kriminelle die Vorzüge der Wolke für sich entdeckt. Der Nachrichtenagentur Bloomberg zufolge sollen Ganoven die Computer von Amazon dazu genutzt haben, um Sony anzugreifen. Hacker haben von den Festplatten des Unterhaltungselektronik-Konzerns aus Japan jüngst Daten von mehr als 100 Millionen Kunden geklaut.

Das alles erstaunt nicht. Der Hype ums Clouden erstaunt ebensowenig wie die Leichtigkeit, mit der nach dem jüngsten NSA Abhörsskandal zur Normalität übergegangen wird. Big Brother im Wohnzimmer, Big Brother in der Luft, Big Brother ominipräsent im Weltnetz. Das alles ist Normalität wie der Milchkaffee zum Frühstück.

Deshalb werden wohl immer mehr Private und Unternehmen sich ins Cloud Computing stürzen. Egal, ob die Daten sicher sind dort, egal, ob man sich auf die Provider verlassen kann. Hauptsache es klingt cool, ist praktisch, reduziert Kosten.

8.86 Anleitung einer sicheren Cloud-Alternative

Provisorische Anleitung einer sicheren Cloud-Alternative von „Nazi-Wähler". Vielen Dank für die Tipps und Grüße nach Meck-Pomm

Okay, bevor ich jetzt als Meckerkopp und Hosenschisser vor allem Neuen dastehe, hier kurz eine Anleitung, wie ich zum Beispiel hochsensible Daten sicher von Meck-Pomm nach Bayern transferiere, ohne dass NSA, BND & Co auch nur den Hauch eines Schimmers haben.

Wenn man keinen eigenen Webspace hat, dann kann man sich den mieten. 5 GB gibt es schon für schlappe 1,49 Euro im Monat, 15 GB schon für 2,49 Euro und ich finde, soviel sollte mir die Sicherheit meiner Daten schon Wert sein.

www.webhostervergleich.org

Wenn man dann seinen Webspace hat, bekommt man von seinem Webhoster die Zugangsdaten zum Server. Nun braucht man noch ein FTP-Programm, was es meist gratis mit dazu gibt, ansonsten: www.filezilla.de

Ein Handbuch oder zumindest eine für Laien verständliche Anleitung, wie man seine Website UND AUCH ANDERE DATEN auf den Server und wieder runter bekommt, ist mit Sicherheit auch im Päckchen bei der Bereitstellung durch den Webhoster dabei, so dass selbst jemand, der nun gar keine Ahnung hat, in der Lage sein müsste, innerhalb von ein bis zwei Stunden seinen eigenen Webserver einzurichten. Jemand, der genau liest und sich an die Vorgaben im Handbuch hält, schafft das in zehn Minuten, ich als Profi in nur ein bis zwei Minuten.

Nun kann man seine schöne selbstgebaute Website ins Internet stellen und sie der ganzen Welt präsentieren oder sich auch fürchterlich vor ihr blamieren. Ich kann das tun, muss ich aber nicht, denn ich kann den Serverplatz auch ganz allein als externen Datenspeicher oder für den Datentransfer benutzen.

Damit niemand merkt, dass es sich um einen reinen Datentransferserver handelt, sollte ich noch eine möglichst dumme und belanglose Website, zum Bleistift von meinem Lieblingslokal, darauf ablegen. Damit wird diese Domain dann schon einmal von den meisten Suchmaschinen als belanglos eingestuft und nicht weiter verfolgt, denn für selbstgemachte Tomatensuppe und Bauernfrühstück interessieren sich weder BND noch NSA.
Wenn dann meine Website endlich komplett steht, kann ich mich wieder mit meinem FTP-Programm auf den Server einwählen und dort beliebig viel Ordner anlegen und auch VERSTECKEN, in denen ich die sensibelsten Daten ablegen kann. Vorzugsweise vom USB-Stick in einem Internetcafé und nicht von zuhause, vom Rechner der eh schon beschnüffelt wird. Dann bitte peinlichst genau darauf achten, dass der Link zu diesem Ordner nirgends verschickt wird, weder per Internet, noch per eBrief, noch per Brief oder Telefon.

Nun verbindet man sich per VPN-Tunnel oder per Fernwartung mit dem Rechner des Empfängers, was sich hiermit besonders gut macht:

www.teamviewer.com

Ich empfehle die portabel Version, da man die mitsamt Einstellungen auf dem USB-Stick mit ins Internetcafé nehmen kann und sie keine auslesbaren Spuren auf dem Rechner hinterlässt.

Wenn ich dann jetzt die Bedienung des Empfängerrechners übernommen habe, dann kann ich diesen mittels FTP-Programm mit dem Server verbinden und die Daten sozusagen ungefährlich und spurenlos am „anderen Ende des Internets“ beim Empfänger ablegen.

Man kann seine Daten auch über längere Zeit dort lagern, denn das Gefährliche ist nicht die Nutzung des Internets als Datenspeicher, sondern die Weitergabe der Links, denn die werden zuerst nachverfolgt und durchschnüffelt.

Eine Dropbox oder Cloude funktionieren nicht viel anders, nur dass den „komplizierten“ (aber auch sicheren) Teil dann schon die anderen übernehmen und wer verschlüsselte Dateien da hoch lädt, macht schon einmal auf sich aufmerksam, noch dazu wenn er dann die Links durch die Welt postet, denn die landen zu allererst bei NSA und BND.

8.87 eBrief Verschlüsselung

Wie wichtig eine abhörsichere Kommunikation ist, kann am Beispiel der Enigma demonstriert werden. Welche geschichtlichen Konsequenzen es haben kann, wenn der Feind die Nachrichten entschlüsseln und in Klartext lesen kann, verdeutlicht der Absatz „Geschichtliche Konsequenzen“ desselben Artikels. Die übliche Übermittlung eines eBrief geschieht unverschlüsselt und kann von jedermann gelesen oder verändert werden. Die Übermittlung der Nachricht geschieht ähnlich einer Postkarte im wirklichen Leben. Das Geschriebene wird auf einem Stück Papier ohne Umschlag weitergereicht und kann folglich von jedem, der die Postkarte in die Hand nimmt, gelesen oder auch verändert werden. Die Übermittlung der Nachricht per Rechner geschieht auf eine ähnliche Weise, die Nachricht wird einfach in Klartext von Server (Rechner im Weltnetz) zu Server weitergegeben, bis sie den Empfänger erreicht hat. Um einen eBrief sicher - ohne dass jemand mitlesen kann- zu übermitteln, muss somit die Nachricht verschlüsselt werden.

Die Verschlüsselung ist also der Umschlag für die Postkarte. Auch die Anhänge an einem eBrief können auf die Weise verschlüsselt übertragen werden.

Es gibt seit längerem für die sichere Kommunikation über den eBrief ausgereifte Verfahren und benutzerfreundliche Programme. Als abhörsicherer Standard hat sich GnuPG durchgesetzt. Das

Programm ist für alle Betriebssysteme verfügbar und der Programmtext liegt offen vor, was heißt, dass keine Hintertürchen oder allgemeingültige Schlüssel eingebaut sind. Somit entspricht das Programm dem Grundsatz jeder Verschlüsselung, wonach „die Sicherheit eines Kryptosystems“ nicht von der Geheimhaltung des Algorithmus abhängen darf. Die Sicherheit darf sich nur auf die Geheimhaltung des Schlüssels gründen.

Um eBriefe verschlüsseln zu können, werden einige kleine aber mächtige Programme benötigt, die nach erfolgreicher Einrichtung das Versenden von sicheren eBriefe bewerkstelligen. Thunderbird ist dabei der Klient der die Nachrichten versendet. GnuPG ist ein freies Programm und übernimmt die eigentliche Ver- und Entschlüsselung unseres eBriefes.

Es gibt tatsächlich einen Pferdefuss - in einem Punkt ist das PGP-System leicht angreifbar, aber auch leicht zu schützen, wenn man weiß, wie.

Wir haben oben gesagt, dass der Vorteil des public-key-Verfahrens darin liegt, dass man seinen Verschlüsselungs-Schlüssel, also den, den die anderen bekommen, nicht geheimhalten muss. Der Nachteil ist die Kehrseite davon: Ein PGP-Schlüssel ist ganz einfach zu fälschen!

Er ist ja nur an seiner Bezeichnung, seiner User-ID, erkennbar, die aus Name und E-Mail-Adresse des Schlüsselinhabers besteht. Und diese beiden Angaben werden bei der Schlüsselherstellung ganz normal eingetippt. Jeder kann daher Schlüssel unter einem beliebigen Namen erstellen.

Daher kannst du dich zunächst einmal nicht darauf verlassen, dass ein Schlüssel wirklich echt ist - außer du warst bei der Erzeugung dabei und hast ihn selbst transportiert.

8.88 Installation von Thunderbird

Zu allererst wird Thunderbird installiert damit du deine eBriefe von deinem eBrief-Anbieter direkt auf dem Rechner verwalten zu kannst.

Dazu lädst du Thunderbird direkt von der Entwicklerseite herunter.

Hier gezeigte Programmversion: 17.0.8

Nach einem Doppelklick auf die Thunderbird Setup 17.0.8.exe öffnet sich das Installationsfenster.

Im nächsten Schritt lässt du alles so eingestellt wie es ist, Weiter.

Mit einem klick auf Installieren beendest du das Installationsfenster und Thunderbird startet das erste mal.

8.89 Einrichtung von Thunderbird

Als ersten Schritt fragt dich Thunderbird ob du Daten und Einstellungen vom vorinstallierten Outlook Express übernehmen möchtest was du verneinst.

Nach dem Start des Programms wirst du gefragt ob du eine neue eBrief Adresse anlegen, oder deine alte benutzen möchtest. Wir Überspringen dies uns nutzen unsere eigene Adresse.

Jetzt bekommst du ein Fenster angezeigt, was dir bei der Einrichtung hilft. Dort gibst du deinen Namen, die zu verwendende eBrief Adresse und das zugehörige Passwort ein und bestätigst mit

Weiter

Nun versucht Thunderbird anhand einer Datenbank herauszufinden, welches die richtigen Server sind und trägt sie bei Gelingen gleich ein. Es kann aber auch passieren, dass nicht die richtigen gefunden werden. In diesem Fall klickst du auf „Bearbeiten“ und gibst die richtigen Server ein.

Der „Posteingangs-Server“ kann entweder ein IMAP-Server oder ein POP3-Server sein, der Postausgangs-Server ist immer ein SMTP-Server. Der Unterscheid zwischen IMAP und POP3 ist, das bei IMAP die Nachrichten direkt auf dem Server verwaltet werden, also demnach immer auf dem Server bleiben, und bei POP3 die Nachrichten in der Regel komplett heruntergeladen werden. Wobei aber Thunderbird die Möglichkeit bietet, die Nachrichten entweder für einen bestimmten Zeitraum oder für immer auf dem Server zu belassen.

Die richtigen Server findest du in der Regel bei deinem eBrief Anbieter oder in dieser Liste. Solltest du immer noch nicht fündig geworden sein, dann hilft nur noch die Benutzung der Suchmaschine deines Vertrauens. Verwende dabei den Namen deines Anbieters und Stichwörter wie POP, POP3, IMAP, SMTP oder Mail-Server. Die Zahlen dahinter werden „Ports“ genannt und sind meist auch bei den entsprechenden Anbietern zu finden.

Hinter den Zahlen steht dann sowas wie „SSL/TLS“ oder „STARTTSL“, welches Verschlüsselungsmethoden sind die aber nur den Weg einer Nachricht vom Klient (Thunderbird) zum Server (Dein Anbieter) verschlüsselt senden. Sobald aber der Server die Nachricht an den Empfänger weiterleitet kann wieder jeder mitlesen, was wir schreiben. Welche Methoden wir nutzen wollen oder können ist jedem selbst überlassen oder wird vom Anbieter vorgeschrieben. Nicht jede Methode wird von den eBrief Anbietern angeboten. Da hilft nur testen. Bestätige mit Fertig deine Einstellungen.

8.90 Was ist PGP/GnuPG/OpenPGP?

PGP (Pretty Good Privacy) wurde von Phil Zimmermann entwickelt um allen Personen die Möglichkeit zu geben, ihre Privatsphäre zu schützen. Die im Folgenden verwendete Open-Source Version des Programms wurde unter dem Namen GnuPG von Werner Koch entwickelt. Um die Interoperabilität zu gewährleisten wurde das von PGP verwendete Dateiformat festgehalten und Erweiterungen definiert. Dieses Format nennt sich OpenPGP und wird von PGP und GnuPG größtenteils eingehalten. PGP und GnuPG ist für viele Plattformen verfügbar, wie z.B. DOS, Windows, Macintosh oder Unix.

Das Verfahren von PGP und GnuPG beruht auf einem Public Krypto Keysystem. Die Ver-/ Entschlüsselung wird mit Hilfe der zwei Schlüssel realisiert: öffentlichem und geheimen. Diese beiden Schlüssel zusammen bilden ein Schlüsselpaar. Mit dem öffentlichen Schlüssel kann die Nachricht an den Besitzer des geheimen Schlüssels nur verschlüsselt werden. Entschlüsselt werden kann diese Nachricht nur mit dem geheimen Schlüssel. Der öffentliche Schlüssel kann nach Belieben und frei verteilt werden. Der geheime Schlüssel muss dagegen auf das Sorgfältigste aufbewahrt werden.

8.91 Was kann GnuPG?

GnuPG ist ein Programm, das primär der Verschlüsselung des Klartexts von eBriefen, Instant Messaging Chats und Kurznachrichten in Ciphertexte dient, so dass nur Sender und Empfänger einer Nachricht, die im Besitz der passenden Schlüssel sind, den Ciphertext wieder in lesbaren Klartext entschlüsseln können. Neben der Nachrichtenverschlüsselung wird GnuPG auch zur Verschlüsselung von Dateien verwendet, die zum Beispiel lokal auf der eigenen Festplatte gespeichert

sind.

Darüber hinaus kann man mit GnuPG Klartexte, Dateien oder Programme mit einer digitalen Signatur versehen, um auch im elektronischen Bereich, in dem eine handschriftliche Unterschrift nicht möglich ist, die Überprüfung der Authentizität elektronisch vorliegender Texte und Daten zu ermöglichen.

Sowohl zur Verschlüsselung als auch zur Signierung setzt GnuPG mathematische Verschlüsselungsfunktionen ein -kryptografische Algorithmen, die in der Welt der Kryptografie als anerkannt sicher vor Entschlüsselung, bzw. Errechnen der originalen Daten.

(z. B. des Klartexts einer EBrief) aus der verschlüsselten Form durch nicht autorisierte, dritte Parteien eingestuft werden. Ein kurzer Blick auf die Struktur und Funktionsweise des Weltnetzes reicht aus, um sich die Notwendigkeit der Verschlüsselung und Signierung vor Augen zu führen.

Beispiel eBrief Überwachung

Wenn ein eBrief versendet wird, werden die Datenpakete des eBriefes zum Mailserver des Providers übertragen, von dort versendet der Mailserver den eBrief an den Ziel-Mailserver des Empfängers. Dabei wird der eBrief meistens mehrere Rechner im Internet passieren, bis dieser am Zielserver ankommt. Der Mailserver des Empfängers überträgt schließlich den eBrief auf den Rechner des Empfängers. Während des ganzen Transportweges werden die Datenpakete stets in lesbarem Klartext übertragen.

Das heißt an verschiedenen Stationen des Weges kann der eBrief abgefangen und auch verändert werden: Auf dem Weg vom eigenen Rechner zum Mailserver, zwischen den einzelnen Rechnern während des Transportes und vom Ziel-Mailserver zum Empfänger. Verschafft sich eine Person einen illegalen Zugang zu einem der beteiligten Rechner, kann auch dort direkt der eBrief abgefangen werden. Zu diesem Zweck gibt es spezielle Programme wie die Paket-Sniffer, mit denen Datenpakete abgefangen werden können. Die abgefangenen Pakete können auch in ihrem Inhalt verändert und wieder in den Datenstrom eingespeist werden.

Zusätzlich können Geheimdienste und Polizeibehörden aufgrund gesetzlicher Befugnisse und mit richterlicher Erlaubnis eBriefe von dem Provider, der den Mailaccount zur Verfügung stellt, zu Überwachungszwecken anfordern.

8.92 eBrief - Verschlüsselung mit GnuPG

Im Folgenden möchten wir dir nur die wesentlichen Funktionen von GnuPG erläutern, ohne dabei aus unserer Sicht unwichtige Funktionen und Anwendungen näher zu beleuchten. Wir nutzen in unserem Leitfaden nie die Funktion der Zwischenablage, sondern vielmehr den Dateimanager. Wir werden auch nicht auf die technischen Hintergründe verschiedener Anwendungen eingehen, sondern dir nur kurz und knapp den Umgang bzw. die Nutzung mit GnuPG zum sicheren Datenverkehr unter Kommunikationspartnern aufzeigen.

Für uns als nationale Sozialisten, die unter permanenter staatlicher Beobachtung stehen, ist es von enormer Bedeutung, einen verhältnismäßig sicheren E-Post-Verkehr gewährleisten zu können. Auch linke Kreise bedienen sich dieser Verschlüsselung und der BRD-Apparat hat große Schwierigkeiten diese Verschlüsselung zu knacken und somit Informationen über die politische Opposition zu sammeln. Die 100%ge Sicherheit im Weltnetz bzw. dem elektronischen Datenverkehr kann und wird es nie geben. **Man muss leider immer von der Möglichkeit ausgehen, dass der Feind mit liest.Machen wir es ihm aber möglichst schwer ... und nutzen daher GnuPG!**

8.93 Installation und Vorbereitung

Eine Bemerkung vorweg: Das hier behandelte Verschlüsselungstool heißt GnuPG (Gnu Privacy Guard). Die dazugehörige graphische Benutzeroberfläche nennt sich WinPT (Windows Privacy Tools). Im Folgenden wird der Einfachheit halber immer von GnuPG gesprochen.

Hier gezeigte Programmversion: 4.5.0

Die von uns verwendete Version kannst du unter www.gnupt.org runterladen.

Nachdem du das Archiv entpackt hast startet die Installation mit einem Doppelklick auf der Datei. Wähle natürlich die Sprache Deutsch.

Klicke auf Weiter und im darauffolgendem Fenster Akzeptierst du die Nutzungsbedingungen und bestätigst mit Weiter. Die Information kannst du auch mit Weiter hinter dich bringen.

Nun wähle das Zielverzeichnis, in das du GnuPG installieren möchtest, aus. Mit einem Klick auf Weiter bestätigst du und es öffnet sich ein kleines Fenster das dich fragt ob du den Ordner erstellen möchtest. Dies bestätigst du mit Ja

Als nächstes musst du das Zielverzeichnis für deine Schlüsselringe wählen. Dieses sollte aus Sicherheitsgründen nicht in das Verzeichnis gelegt werden, in dem auch GnuPG installiert wurde. In diesem Ordner werden dann zukünftig dein noch zu erstellendes Schlüsselpaar und die öffentlichen Schlüssel deiner Kommunikationspartner abgelegt sein.

Wähle die vollständige Installation aus. Setze im darauffolgendem Fenster die Haken bei allen zusätzlichen Aufgaben auswählen. GnuPG wird dann zukünftig automatisch beim Start deines Rechners in der Task-Leiste angezeigt.

Nach dreimaligen klicken auf Weiter Installierst du das Programm nun auf deinem Computer.

Ist die Installation beendet drückst du auf Weiter und im nächsten Fenster auf Fertigstellen.

Bevor du mit GnuPG eBriefe ver- und entschlüsseln kannst, musst du dir ein Schlüsselpaar generieren. Dieses besteht aus einem sog. öffentlichen und einem privaten Schlüssel. Verschlüsselt wird immer mit dem öffentlichen Schlüssel des Empfängers, den der Empfänger zum Beispiel per eBrief zugesandt hat und der sich nach dem Import jetzt im eigenen Schlüsselring befindet. Der Empfänger benutzt zum entschlüsseln des eBriefes seinen privaten Schlüssel.

Da du noch kein Schlüsselpaar besitzt, fragt GnuPG, ob der Schlüsselerzeugungs-Dialog gestartet werden soll.

Fülle nach einem Klick auf Ja die Felder der Eingabemaske entsprechend aus:

Bei Name solltest du den Namen wählen, unter den du zukünftig kommunizieren willst. Gleiches gilt für die E-Brief-Adresse.

Nun musst du ein Passwort wählen.
Bitte Abschnitt Das Passwort beachten!

Weiter!

Der Schlüssel wird nun erzeugt.

Nach Abschluss der Schlüsselgenerierung bietet das Programm an, Sicherungen der gerade erzeugten Schlüssel zu erstellen. Folge den Anweisungen und speichere sowohl den öffentlichen als auch den privaten Schlüssel sicher ab. Danach schließt du das Fenster mit Klick auf Ende.

Zur Verschlüsselung wird ein Verfahren namens RSA verwendet, mit einer Schlüssellänge von bis zu 4096 Bit. Schlüssel in dieser Länge sind aufgrund der hieraus entstehenden Kombinationsmöglichkeiten und dem daraus resultierenden technischen Aufwand für die Entschlüsselung nicht in annehmbarer Zeit zu knacken. Ein Versuch, einen 640 Bit -(etwa 72 Bit symmetrisch) langen Schlüssel zu knacken, dauerte mit 80 Rechnern à 2,2 GHz rund 10 Monate. Der 4096 Bit - (etwa 200 Bit symmetrisch) Schlüssel hat $3,4^38$ (also 34 mit 37 Nullen dahinter) mehr Variationen. Die Entschlüsselungszeit wird um denselben Faktor länger. Somit ist die Verschlüsselung an sich sehr sicher und wird in den nächsten Jahrzehnten auch sicher bleiben. Vorausgesetzt natürlich, dass der geheime Schlüssel zum Entschlüsseln nicht entwendet wird. Der ist allerdings mit einem Passwort geschützt, welches verständlicherweise gut gewählt sein sollte.

8.94 Eigenen öffentlichen Schlüssel versenden

Die Schlüsselverwaltung von GnuPG erreichst du fortan über eine Desktopverknüpfung oder über ein kleines Schlüsselymbol in der Task-Leiste.

Starte die Schlüsselverwaltung entweder durch Doppelklick auf das Schlüssel-Icon oder wähle nach einem Rechtsklick den entsprechenden Menüpunkt aus.

Wähle dein eigenes Schlüsselpaar aus (gekennzeichnet durch Typ pub/sec) und drücke die rechte Maustaste und wähle anschließend Sende Schlüssel an Mail-Empfänger.

Dein öffentlicher Schlüssel wurde nun automatisch an einen eBrief (z.B. im Thunderbird) angehängt. Wenn das nicht gehen sollte

Eigenen Schlüssel anklicken, im Menu Schlüssel auswählen und Exportieren wählen. Anschließend den eigenen öffentlichen Schlüssel abspeichern und als Dateianhang an den Kommunikationspartner versenden.

Dein Kommunikationspartner wird dann zukünftig Nachrichten an dich mit deinem eigenen öffentlichen Schlüssel verschlüsseln.

-Fremden öffentlichen Schlüssel importieren

Starte die Schlüsselverwaltung durch Doppelklick auf das Schlüssel-Icon oder wähle nach einem Rechtsklick den entsprechenden Menüpunkt auf.

Hier kannst du sehen, mit wem du die Schlüssel ausgetauscht hast, ob diese noch gültig sind und du bekommst einen Überblick über Stärke und Typ der Schlüssel. Im Moment sieht das Ganze noch etwas trostlos aus. Du hast nur einen einzigen Schlüssel: Deinen eigenen.

Um mit einem Partner verschlüsselte eBriefe auszutauschen, benötigst du dessen öffentlichen Schlüssel. Den bekommst du normalerweise direkt von ihm per eBrief oder auf einen Datenstift oder von einem Schlüsselserver. Dabei handelt es sich um Rechner im Weltnetz, an die jeder seinen öffentlichen Schlüssel schicken kann. Von dort kann sich dann ein Kommunikationspartner den Schlüssel herunterladen, auch wenn der Besitzer gerade im Urlaub ist.

Normalerweise erhälst du einen öffentlichen Schlüssel per eBrief mit einem Dateianhang (Format asc). Dieser Dateianhang ist der öffentliche Schlüssel des Kommunikationspartners und dieser

öffentliche Schlüssel muss in die eigene Schlüsselverwaltung importiert werden. Zukünftig wirst du nun alle Nachrichten an diesen Kommunikationspartner mit seinem öffentlichen Schlüssel verschlüsseln. Dieser kann dann nach Erhalt der verschlüsselten Nachrichten mit seinem dazugehörigen privaten Schlüssel die an ihn mit seinem öffentlichen Schlüssel verschlüsselten Nachrichten entschlüsseln. Man verwendet also immer das eigene Schlüsselpaar, bestehend aus öffentlichen und privaten Schlüssel, zur sicheren Verschlüsselung.

Zuerst speicherst du den erhaltenen öffentlichen Schlüssel in dem bei der Installation gewählten Ordner für die Schlüsselpaare ab.

Nun öffnest du die Schlüsselverwaltung. Du Startest entweder die Schlüsselverwaltung durch Doppelklick auf das Schlüssel-Icon oder wählst nach einem Rechtsklick den entsprechenden Menüpunkt aus.

Jetzt öffnest du den Menüpunkt Schlüssel, Importieren und fügst den erhaltenen Schlüssel hinzu.

Mit einem Klick auf Importieren wird der Vorgang abgeschlossen. Du hast somit den öffentlichen Schlüssel des Kommunikationspartners in deinem Schlüsselbund aufgenommen.

8.95 Dateien verschlüsseln und versenden

Schreibe die Nachricht, welche du an den Kommunikationspartner versenden möchtest, entweder in einem Word-Dokument oder in einem reinen Textdokument. Dann speichere es ab und schließe die Datei.

Starte den Dateimanager durch einem Rechtsklick auf das Schlüssel-Icon in der Task-Leiste und rufe den entsprechenden Menüpunkt auf.

Schiebe (per Drag and Drop) die eben abgespeicherte Datei in den Dateimanager hinein.

Dann die Datei anwählen und über den Menüpunkt Datei, Verschlüsseln verschlüsseln.

Nun wird man gefragt, an wen man alles diese Nachricht versenden möchte. Setze entsprechend deinen gewünschten Kommunikationspartnern den Haken. Drücke anschließend OK und beantworte die folgenden Fragen mit Nein.

Hierbei können mehrere Kommunikationspartner ausgewählt werden. All diese können dann in Verbindung mit ihrem eigenen privaten Schlüssel deine mit ihren öffentlichen Schlüssel verschlüsselte Nachricht öffnen.

Die verschlüsselte Datei wird unter dem gleichen Verzeichnis abgespeichert aus der man auch die zu verschlüsselte Datei gewählt hatte.

Mit dieser Vorgehensweise lassen sich sämtliche Datei-Formate verschlüsseln.

Anschließend noch die verschlüsselte Datei an den eBrief anhängen und an die ausgewählten Kommunikationspartner versenden.

8.96 Dateien entschlüsseln

Den Anhang (verschlüsselte Datei) des erhaltenen eBriefes des Kommunikationspartners in einem Verzeichnis ablegen. Mit einem Doppelklick auf die verschlüsselte Datei öffnet sich ein Fenster.

Dein eigenes Passwort eingeben und die Datei wird entschlüsselt im gleichen Verzeichnis wo ebenfalls die verschlüsselte Datei abgelegt ist.

Sollte dies nicht funktionieren
Einfach die verschlüsselte Datei (per Drag & Drop) in den Dateimanager schieben und dort entschlüsseln. Dein eigenes Passwort eingeben und die Datei wird entschlüsselt im gleichen Verzeichnis wo ebenfalls die verschlüsselte Datei abgelegt ist.

8.97 Sinn und Legitimität der GnuPG-Verschlüsselung

Nach soviel Anstrengung, eMails wirklich mitlessicher zu machen, wirst du dich vielleicht fragen, ob dies nicht vielleicht ein bißchen hysterisch ist. Es mag vielen Leuten möglicherweise so vorkommen, weil sie ja „nichts zu verbergen“ haben. Aber es gibt sehr stichhaltige Argumente dagegen: Zwar weiß jeder, was man üblicherweise in den diversen Kabinen einer öffentlichen Toilette tut, aber es ist trotzdem absolut üblich, die Tür zu verriegeln. Klar, es wird dort mitunter auch Mißbrauch wie z.B. Drogenkonsum getrieben, aber trotzdem lassen Sie es sich sicherlich auch bei bestimmungsgemäßem Gebrauch nicht verbieten, die Tür abzuschließen. Vom deutschen Gesetzgeber wird Ihnen ja auch ausdrücklich das Recht auf Privatsphäre zugesichert.

Kaum jemand wird auf die Idee kommen, fremden Leuten unnötig Einblick ins eigene Privatleben zu gewähren, d.h. im ganz normalen Leben mashdt du von diesem Recht meistens ausgiebig Gebrauch, ohne groß darüber nachzudenken. Man denke nur an die Diskretion eines Kreditinstituts (Dein Nachbar muß ja nicht wissen, wieviel Geld oder Schulden Du hast), abschließbare Briefkästen, Gardinen, Sichtschutz für den Balkon/Garten und vieles mehr. Aus diesem Grund möchten wir dich dazu ermuntern, sich nicht im Internet als gläserner Surfer zu bewegen. Denn aus deinen eMails kann man sehr leicht z.B. ein Profil von dir anfertigen. Eine Bombardierung mit „zielgruppenorientierter“ Werbung wäre dann noch die harmloseste Konsequenz. Bitte bedenke, dass Ihre Kommunikation per ganz normaler Post recht gut vor neugierigen Blicken geschützt ist. Erst nach richterlicher Anordnung dürfen Ermittlungsbehörden deine Briefe öffnen. Ähnliches gilt für Telefongespräche, wobei hier jedoch bekannterweise die NSA (National Security Agency, d.h. der amerikanische Geheimdienst) illegalerweise fast alles mithört.

Es ist sinnvoll, sein ganz legales und vor allem legitimes Recht auf Privatsphäre vor allem im Internet wirklich auch zu nutzen. Denn hier ist es viel einfacher, dich -zu welchem Zweck auch immer- auszuspionieren, weil die Daten ja schon gleich in digitaler Form vorliegen und in tausendstel Sekunden ausgewertet werden können. Zudem könnte der Gesetzgeber auf die Idee kommen, dass er die Privatsphäre im Internet problemlos einschränken könne, weil ohnehin nur sehr wenig Leute Gebrauch von ihrem Grundrecht machen. Eine Firma sollte ohnehin ihre gesamte Korrespondenz mit den Geschäftspartnern ausschließlich verschlüsselt abwickeln, weil bekanntermaßen die NSA (und nicht nur die!) u.a. durch Auswerten von eMails Wirtschaftsspionge betreibt. Leider wird dies von fast allen Firmen sträflichst vernachlässigt. Es ist daher kein Wunder, wenn so manches erfolgversprechender Geschäftsabschluß in letzter Minute platzt, weil ein Konkurrent Informationen besitzt, die ihn in die Lage versetzen, ein attraktiveres Angebot zu machen.

8.98 Installation der Erweiterung Enigmail für Thunderbird

Um Enigmail zu installieren gibt es zwei Möglichkeiten. Die eine Möglichkeit erfolgt direkt über Thunderbird. Dazu startest du Thunderbird wieder und rufst, oben rechts, über das Anwendungsmenü den Add-on-Manager auf.

Es hat sich nun der Add-ons-Manager geöffnet und du gibst in das Suchfeld Enigmail ein und bestätigst mit Enter.

An der ersten Stelle ist auch schon das gesuchte Add-on. Nach einem Klick auf Installieren läd Firefox das kleine Helferlein herunter und installiert es.

Nach der Installation muss Thunderbird neu gestartet werden damit das Add-on aktiv wird.

Du kannst Enigmail aber auch direkt herunterladen und es dann über „Installieren“ in der Add-On-Verwaltung auswählen und installieren.

8.99 Allgemeine Einstellungen von Enigmail

Nachdem Thunderbird neugestartet wurde siehst du in der Menüleiste einen neuen Reiter mit dem Namen OpenPGP über den wir nun die „Einstellungen...“ öffnen.

Jetzt wird dir der „OpenPGP-Assistent“ angezeigt welchen du durch einen Klick auf „Abbrechen“ beendest. In den Einstellungen stellst du nun sicher, dass der Pfad zu GnuPG der richtige ist. Das bewerkstelligst du, indem du dem Pfad zur Anwendung folgst und dort eine gpg.exe auffindest.

Windows XP: C:/Programme/GNU/GnuPG/gpg.exe
Windows Vista: C:/Program Files/GNU/GnuPG/gpg.exe
Windows 7: C:/Program Files/GNU/GnuPG/gpg.exe

Sollte diese dort nicht zu finden sein, solltest du dich besinnen wo du GnuPG installiert hast. Wenn du also den Pfad bei der Installation von GnuPG geändert hast, findest du es dann auch in dem entsprechenden Pfad und suchst dir diesen, nachdem du das Kästchen „Anderer Pfad“ aktiviert hast. Nun setzt du noch die Zwischenspeicherung des Passworts auf „0 Minuten“, damit innerhalb von 5 Minuten nach der Passwort-Eingabe niemand deine Verschlüsselten Nachrichten ohne erneute Passwort-Eingabe lesen kann und bestätigst die Einstellungen mit „OK“.

8.100 Erzeugen eines Schlüssels

Rufe nun über „OpenPGP ≫ Schlüssel verwalten“ die Schlüsselverwaltung auf.

In dieser gehst du dann auf „Erzeugen ≫ Neues Schlüsselpaar“. Wieder wird ein neues Fenster angezeigt. In diesem Fenster trägst du nun zweimal ein sicheres, neues Passwort ein, aktivieren das Kästchen SSchlüssel läuft nie abünd erzeugen unser Schlüsselpaar mittels Klick auf „Schlüsselpaar erzeugen“. Bitte Abschnitt Das Passwort beachten!

Nach nochmaligem bestätigen wird der Schlüssel erstellt. Wenn nun die Bestätigung anzeigt, dass der Schlüssel erzeug wurde, wird gleichzeitig gefragt ob du ein Widerrufszertifikat erzeugen willst.

Dies bestätigst du mit „Zertifikat erzeugen“, speicherst es vorerst auf dem Rechner, musst dann dein Passwort eingeben was du zur Erzeugung des Schlüssels verwendet hast und bekommst wieder eine Bestätigung, die du mit „OK“ wegklickst.

Durch Aktivieren des Kästchens „Standardmäßig alle Schlüssel anzeigen“ wird dein Schlüssel angezeigt und du exportierst diesen mittels Rechtsklick und „In Datei exportieren“.

Im neuen Fenster wählst du „Geheime Schlüssel exportieren“ und speichern den Schlüssel dort wo auch das Widerrufszertifikat liegt.

Beide Dateien sollten an einem sicheren Ort, wie einer veschlüsselten Festplatte, gespeichert werden. Zwar kann mit dem Schlüssel niemand was anfangen solange er nicht das Passwort deines Schlüssels weiß, aber man kann sich nicht genügend absichern.

8.101 Versenden und Empfangen verschlüsselter eBriefe

Um nun einen verschlüsselten eBrief zu verschicken klickst du in Thunderbird auf „Verfassen“. Nun öffnet sich ein neues Fenster, in dem du die Empfänger-Adresse eingibst, den Betreff und deine Mitteilung, die den Empfänger erreichen soll. Zum Betreff sollten wir aber wissen, dass dieser NICHT verschlüsselt wird. Das heißt dort verwenden wir entweder belanglose Betreffs oder aber irgendwelche Floskeln. Auf jeden Fall nichts was inhaltlich mit der eigentlichen Nachricht zu tun hat.

Wenn du nun noch niemanden hast dessen Schlüssel du auch besitzt kannst du logischerweise noch niemandem verschlüsselte Nachrichten schicken. In dem Fall testen wir das Ganze in dem wir uns selbst als Empfänger eintragen.

Bisher werden die eBriefe aber noch unverschlüsselt versendet. Um das zu ändern gibt es in diesem Fenster einen weiteren OpenPGP-Knopf den du anklickst und am besten alle Kästchen aktivierst die im neuen Fenster angezeigt werden.

Ersteres unterschreibt deine Nachricht, sodass der Empfänger sicher weiß dass die Nachricht wirklich vom Absender ist. Das zweite Kästchen aktiviert die eigentliche Verschlüsselung und das dritte formatiert die Nachricht im eigenen PGP/MIME-Standard. Nun schickst du die Nachricht über „Senden“ auf den Weg in die weite Welt. Bevor die Nachricht aber abgesendet wird musst du das Passwort für den Schlüssel eingeben, nim das Häkchen unter der Eingabe heraus und bestätigen wieder mit „OK“.

Weil wir die Nachricht nun an uns selbst geschickt haben, sollte nach einem Klick auf „Abrufen“ eine verschlüsselte Nachricht eingegangen sein. Diese können wir nun nur öffnen, wenn wir unser Schlüssel-Passwort eingeben.

8.102 Das Problem: Schlüssel Echtheit

Stellen wir uns zwei Leute vor, Anja und Martin. Die wollen sich PGP-Verschlüsselte eBriefe schicken. Anja erzeugt also einen Schlüssel, den wir mal Anja-1 nennen, und schickt ihn per eBrief an Martin. Martin erzeugt auch einen - Martin-1, den er per eBrief an Anja schickt.

So weit die Theorie. Die Schlüssel wurden abgeschickt und liegen auf irgendeinem Mail-Server im Netz. Und jetzt wirds spannend.

8.103 Der „Man-in-the-middle“ Angriff

Nehmen wir mal an, bei Martins eBrief Provider sitzt jemand, der alle eBriefe von und für Martin abfängt und speichert, um Informationen über Martins Privatleben zu sammeln. Der sieht jetzt Martins eBrief mit dem Schlüssel drin und denkt sich: Hoppla, der will seine eBriefe jetzt geheimhalten? Na warte[2]!

Weil dieser Mensch (in Wirklichkeit wird das natürlich ein automatisch arbeitendes Softwareprogramm sein, aber bleiben wir mal dabei) sehr raffiniert ist, blockiert er den Weitertransport des

[2] Bilder auf s-f-n.org

eBriefes (mit dem Schlüssel) an Anja, startet dann PGP auf seinem Computer und erzeugt einen neuen Schlüssel, wobei er als Benutzerkennung Martins Namen und eBriefadresse eingibt (die kennt er ja aus Martins Schlüssel). Nennen wir dieses komplett neue Schlüsselpaar mal Martin-2. In Martins eBrief an Anja ersetzt er den originalen Martin-1-Schlüssel durch den neuen Martin-2 und schickt diesen geänderten eBrief an Anja. Anja freut sich - sie hat wie verabredet von Martin einen eBrief bekommen, in der ein Schlüssel war, der Martins Name und Adresse trägt. Dass der Schlüssel, den sie bekommen hat, nicht der ist, den Martin erzeugt hat, ahnt sie nicht!

Dasselbe macht der Fälscher natürlich auch mit Anjas Schlüssel. Und jetzt mach dir mal klar, wer welche Schlüssel hat. Der „Man-in-the-middle“ (so heißt dieser Fälscher im PGP-Jargon) hat nämlich jetzt schon die komplette Verschlüsselung ausgehebelt!

8.104 Wie dieser Angriff funktioniert

Machen wir es uns an einem Beispiel klar: Anja schickt einen (wahrscheinlich sehr persönlichen) eBrief an Martin, die sie natürlich mit dem Schlüssel Martin-2 verschlüsselt - einen anderen Schlüssel hat sie ja nicht. Der Fälscher fängt den eBrief ab, entschlüsselt ihn (das kann er ja - er hat den private key zu Martin-2), archiviert den Klartext, verschlüsselt ihn wieder mit Martin-1 (er tut also Martin gegenüber so, als wäre er Anja) und schickt das an Martin weiter. Der kann das entschlüsseln, und alles scheint in Ordnung zu sein - keiner der beiden merkt, dass noch ein Entschlüsselungs-Verschlüsselungs-Vorgang dazwischen liegt!

Weil das natürlich auch andersherum geht (mit Anjas Schlüsseln), ist die gewollte Geheimhaltung komplett im Eimer.

8.105 Schlüssel-Integrität ist der Dreh- und Angelpunkt!

Wir hoffen, du bist gedanklich einigermaßen mitgekommen. Es kommt alles darauf an, dass die beiden zuallererst überprüfen, ob der Schlüssel, den sie vom anderen erhalten haben, auch wirklich der ist, den der andere erzeugt hat.

Dass man diese Prüfung nicht per eBrief, sondern auf einem anderen Kommunikationskanal vornimmt, sollte klar, sein, oder? Sonst kann der Man-in-the-middle ja wieder dazwischenfunken ...
Das musst du natürlich nicht jedes Mal machen; es genügt, einen per eBrief empfangenen Schlüssel einmalig auf seine Echtheit zu prüfen. Denn dass der Man-in-the-middle direkt auf Anjas Rechner einen bereits überprüften Schlüssel austauschen kann, ist sehr unwahrscheinlich.

Wie oft ein Man-in-the-middle-Angriff vorkommt, weiss ich nicht. Aber darauf kommt es überhaupt nicht an - dieser Angriff ist die bei weitem leichteste und billigste Methode, ein public-key-Verfahren auszuhebeln. Es ist systembedingt der größte Schwachpunkt von PGP, doch wenn du das Thema ernst nimmst, dann hast du dieses Loch schon gestopft. PGP ist sicher, wenn man richtig damit umgeht. Die Echtheit von Schlüsseln spielt bei PGP also eine (genauer: die) entscheidende Rolle. Gewöhn dir an, niemals einen Schlüssel zu benutzen, von dessen Echtheit du nicht überzeugt bist!

Davon überzeugt sein kannst du auf verschiedenen Wegen, der beste ist die persönliche Überprüfung. Und jetzt willst du bestimmt wissen, wie man das machen kann.

8.105.1 Echtheit von Schlüsseln überprüfen

Das Beste ist natürlich: Die beiden besuchen sich, erzeugen ihre Schlüssel gemeinsam und nehmen sie (auf einem Datenträger, den sie währenddessen nie aus den Augen lassen) mit nach Hause.

Eine weitere Möglichkeit ist: Die beiden schicken sich die Schlüssel zwar per Mail, rufen sich aber dann sofort an und buchstabieren sich gegenseitig die Textversionen (Fingerabdruck) ihrer Schlüssel vor.

„Groß Q klein L klein A Vier Klein Ypsilon Zwei Fünf Klein X Klein f ...“

Du suchst den Fingerabdruck deines Schlüssels? Kein Problem...

Rufe im Thunderbird über „OpenPGP ≫ Schlüssel verwalten“ die Schlüsselverwaltung auf. Mit einem doppelklick auf deinen Schlüssel öffnet sich ein Fenster mit dem Fingerabdruck.

8.106 Nachrichtensofortversand

Eine einfache Möglichkeit direkten Kontakt zu Jemandem aufzunehmen ohne wie bei eBriefen lange warten zu müssen, sind sogenannte Instant-Messaging-Programme. Bei diesen Programmen muss man unterscheiden zwischen Übertragungsprotokoll (Jabber, ICQ, AIM, Skype, IRC, MSN etc.) und der Anwendung an sich.

Zwar bieten die Entwickler eines jeden Protokolls eigene Programme an, jedoch gibt es auch sogenannte Multi-oder Sammelprogramme. Mit ihnen kann man mehrere Protokolle (ICQ-Zugang/Konto, MSN-Zugang/Konto) verwalten, ohne mehrere Programme im Hintergrund laufen zu haben. In diesem Fall entscheiden wir uns für das Programm Pidgin, welches gut konfigurierbar, intuitiv zu steuern und gut erweiterbar mit Verschlüsselungsdiensten ist. Als Protokoll wählen wir zudem das open-source Protokoll Jabber.

Mit Jabber wartet eine mächtige Instant-Messaging-Alternative darauf, ihre Möglichkeiten einem breiten Benutzerkreis zur Verfügung zu stellen. Bis auf einen weniger umfangreichen Funktionsumfang für Multimedia gibt es bei Jabber keinerlei Fallstricke. Die klassischen IM-Netzwerke AIM, ICQ, MSN und Konsorten hinken durch restriktive Lizenzbedingungen bezüglich der Verwendbarkeit alternativer -Clients hinterher. Schwerwiegender sind zudem bedenkliche Nutzungsbedingungen in Bezug auf Rechteübergang für alle über diese kommerziellen Netzwerke gesendeten Daten.

Unbestreitbar bieten die Clients von MSN und AIM zwar gewisse Features, von denen Jabber noch eine gute Ecke entfernt ist, doch wer auf multimediale Funktionen nicht angewiesen ist, ist mit der Kombination von Jabber-Client, Jabber-ID und Transports sicher sehr gut bedient. Ein offenes Protokoll, die mögliche Eigenentwicklung von Protokoll-Erweiterungen sowie eine breite Nutzerbasis verhelfen dazu, Jabber zu den Anbietern der proprietären Messaging-Netzwerke konkurrenzfähig aufzustellen.

Die Aufgabe der Echtzeit-Verschlüsselung der gesendeten Nachrichten übernimmt das Off-The-Record-Plugin.

Off-the-Record Messaging (zu deutsch: inoffizielle; vertrauliche, nicht für die Öffentlichkeit bestimmte Nachrichtenvermittlung) ist ein Protokoll zur Nachrichten-Verschlüsselung von Instant Messaging. Im Gegensatz zur Übertragung der verschlüsselten Nachrichten mittels GPG, PGP (oder in seltenen Fällen auch mittels X.509-Zertifikat) kann man beim Off-the-Record Messaging später nicht mehr feststellen, ob ein bestimmter Schlüssel von einer bestimmten Person genutzt wurde (deniability; Prinzip der Abstreitbarkeit). Dadurch lässt sich nach Beenden der Unterhaltung von niemandem (auch keinem der beiden Kommunikationspartner) beweisen, dass einer

der Kommunikationspartner eine bestimmte Aussage gemacht hat. Umgesetzt wird dieses Prinzip durch kombinierte Verwendung des symmetrischen Kryptoverfahrens AES, des Diffie-Hellman-Schlüsselaustauschs und der Hashfunktion SHA-1. Die beiden Entwickler, Ian Goldberg und Nikita Borisov, stellen eine Bibliothek, ein Plugin für Pidgin sowie einen OTR-AIM-Proxy zur Verfügung. Die Bibliothek ist unter der LGPL lizenziert. Das mit der Bibliothek mitgelieferte Toolkit um Nachrichten zu fälschen, das Pidgin-Plugin und die Proxy-Software sind dagegen unter der GPL lizenziert.

8.106.1 Installation von Pidgin

Bevor wir zur Installation übergehen, solltest du dir erst überlegen, über welchen Jabber-Server du komunizieren willst. Anders als proprietäre Messenger hat Jabber viele verschiedene Server. Die bekanntesten und meist genutzten sind der vom Chaos Computer Club (www.jabber.ccc.de) und der von Jabber.org (www.jabber.org).

Bei der Auswahl des Servers solltest du darauf achten, einen möglichst grossen zu wählen und dass der, den du wählst, SSL unterstützt. Bei kleineren ist die Chance gross, dass sie plötzlich einfach vom Netz gehen. Wir würden dir also empfehlen, den vom CCC oder jabber.org zu nehmen.

Für manche vieleicht interessant: deine Jabber-Adresse (Jabber ID = JID) wird wie eine eBrief-Adresse aussehen, wobei der Server den letzten Teil darstellt. John_Doe@jabber.ccc.de wäre eine hypothetische Beispieladresse.

Hier gezeigte Programmversion: 2.10.7

Zuerst lädst du dir die neuste Version von Pidgin herunter.

Die Installation startet nach einem Klick auf die heruntergeladene Datei: pidgin-2.10.7.exe.

Nach zweimaligen drücken von Weiter machst du in dem Fenster einen Haken in dem Punkt Desktop damit du Pidgin auch wieder findest. Weiter

Hier siehst du den Installationsort für Pidgin. Zur bestätigung drücke auf Installieren.

Pidgin läd jetzt eine benötigte Datei herunter und das Programm wird installiert.

Mit einem klick auf Fertig Stellen beendest du die Installation.

Nachdem du Pidgin über die die Desktopverknüpfung gestartet hast erscheint ein Fenster, welches dich auffordert ein neues Konto zu erstellen. Drücke auf Hinzufügen.

Im folgenden Fenster wählst du XMPP für das Jabber-Protokoll. In das Feld Benutzer kommt logischerweise der Benutzername bei Domain gibst du die Serveradresse ohne http://www ein. Wählst du den Chaos Computer Club sähe die eingabe so aus: jabber.ccc.de. Bei Lokaler Alias kommt dein Benutzernahme rein. Ausserdem musst du unten einen Haken bei: Dieses neue Konto auf dem Server anlegen machen.

Nun möchte Pidgin das du dein Jabber Passwort angibst. Der Haken wird natürlich nicht gesetzt. Pidgin speichert die Passwörter im Klartext auf dem Computer. Somit haben sogenannte „Stealer“ leichtes Spiel das Passwort zu klauen. Wie der Name schon sagt, klauen Stealer alle gespeicherten Passwörter auf dem Computer. Die Datei mit den Zugangsdaten befindet sich unter:

Windows XP:
C:/Dokumente und Einstellungen/„Benutzername“/Anwendungsdaten/.purple

Windows Vista & 7:
C:/Users/„Benutzername“/AppData/Roaming/.purple.
Die Datei heißt „accounts.xml“.

Unser neuer „Instant Messenger“ ist nun fertig Installiert und sieht nun so aus.

Außerdem solltest du unbedingt einstellen,
dass deine Gespräche nicht protokolliert werden

Dazu klickst du auf Werkzeuge und in dem sich aufklappenden Fenster auf Einstellungen.
Auf dem Reiter Mitschnitte nimmst du alle Haken raus.

8.106.2 Einrichten der Nachrichtenverschlüsselung

Durch das Off-The-Record-Plugin erreicht man einen sehr hohen Grad an Sicherheit in Bezug auf die Verschlüsselung.

Hier gezeigte Programmversion: 4.0.0-1

Zuerst solltest du Pidgin beenden. Dann kannst du dir wieder die neuste Version des OTR plugin for Pidgin herunterladen und mit einem Doppelklick öffnen.

Es öffnet sich das Pidgin-OTR Setup. Next. Im nächsten Fester musst du die Lizenbestimmungen akzeptieren und im dritten Fenster siehst du den Installationsort und drückst auf Install.

Nachdem die Installation abgeschlossen ist kannst du nun Pidgin erneut starten und wählst im Menü Werkzeuge und in dem sich aufklappenden Fenster Plugins.

In dem sich öffnenden Fenster suchst du den Eintrag Off-the-Record Messaging 4.0.0 und wählst ihn mit einem Haken an.

Als nächstes drückst du auf Plugin konfigurieren. Hier musst du einen Fingerabdruck erstellen. Dazu klickst du auf Generieren und musst etwas warten. Überprüfe ob die Haken bei Standart OTR-Einstellungen richtig gesetzt sind.

Ist der Fingerabdruck erstellt kannst du mit OK Bestätigen und die Fenster wieder schiessen.

8.106.3 Beginnen einer sicheren Unterhaltung

Deine Kontakte heissen in diesem Programm Buddy.

Beginnst du nun eine Unterhaltung mit einem Kameraden, drückst du oben auf OTR ¿ Private Unterhaltung starten.

Du drückst nun wieder auf ORT ¿ Buddy authentifizieren um sicherzustellen, dass du mit der Person redest welche du auf der Gegenseite annimmst.

In dem Fenster Authentifiziere Buddy musst du nun eine Sicherheitsfrage mit dazugehöriger Antwort erstellen. Die Antwort dürfen natürlich nur der Gesprächspartner selbst und du wissen. Die Anfrage zur Authentifizierung wird mit Authentifizieren abgeschickt.

Du wartst nun auf die Beantwortung deiner gestellten Sicherheitsfrage.

Hat dein Gesprächspartner die Antwort korrekt eingegeben erscheint die Meldung Authentifizierung erfolgreich.

Diese Prozedur muss von beiden Seiten aufgestellt werden, d.h. du musst ebenfalls eine Sicherheitsfrage beantworten.

In dem Gesprächsfenster wird nun auf der rechten Seite Privat angezeigt, die Unterhaltung beginnt ab nun verschlüsselt und authentifiziert, d.h. es sprechen auch wirklich die Personen miteinander für die sie sich ausgeben.

Hinweis:
Beim erneuten Öffnen einer Unterhaltung mit einem schon authentifizierten Gesprächspartner, wird die erste Nachricht, die du dem Gesprächspartner schickst, nicht verschlüsselt. Erst nach dem ersten Senden einer Nachricht wird die Verschlüsselung der Unterhaltung aktiviert. Vorbeugend kannst du vor dem Senden der ersten Nachricht, mittels „OTR -¿ Private Unterhaltung starten“ die Unterhaltung manuell verschlüsselt starten. Daten, also Fotos, Worddateien oder ähnliche, welche man per Pidgin verschicken kann werden nicht Verschlüsselt übertragen!! Du solltest besser einen zuvor erstellten Datentresor an deinen Gesprächspartner schicken und ihm dann das Passwort, welches wieder durch Pidgin verschlüsselt ist, schreiben.

8.107 Suchmaschine gleich Suchmaschine?

Google dürfte wohl die meist bekannteste und zugleich meist verwendete Suchmaschine im Weltnetz darstellen. Google ist aber nicht nur das, sondern auch ein extremer Datensammler. **Vielleicht sogar extremer als so mancher selbsternannter Extremist.**

Das Portal Spiegel-Online schrieb dazu unter anderem folgendes:
Seit Montag protokolliert Google Ihr Suchverhalten auch dann mit, wenn Sie keinen Google-Account haben. Jede Suchanfrage wird gespeichert, 180 Tage lang. Verbunden mit der IP-Adresse und der Kennung Ihres Browsers - also nicht mit Ihrem Namen. Den kennt Google nur, wenn Sie auch noch eine entsprechende Google-Mail-Adresse oder für andere Online-Anwendungen einen Google-Account eingerichtet haben. Ist das der Fall, weiß der Konzern ohnehin sehr viel darüber, was Sie online tun - und zwar ohne Zeitbeschränkung. Und wenn Sie auch noch den Google Chrome Browser oder eine Google Toolbar installiert haben sollten, speichert Google nicht nur alles, wonach Sie je gesucht haben und alle Suchergebnis-Links, die Sie je angeklickt haben, sondern auch noch alles andere, was Sie mit ihrem Browser machen.

Zu der extremen Sammelwut der „Googleaner“ kommt noch hinzu das Google.de im Gegensatz zu Google.com zensiert und streng nach den vorgeschriebenen politisch korrekten Dogmen handelt. Wenn man also überhaupt Google verwenden will, so sollte man die deutschsprachige Google.com Version verwenden, die der Google.de Version in Sachen Suchen in Nichts nach steht. Generell können wir **dem Gebrauch von Google, und da macht es keinen Unterschied ob .com oder .de, aber nur abraten.**

Wir wollen dir stattdessen das Verwenden der folgenden Suchmaschinen ans Herz legen:
www.ixquick.com wird von der niederländischen Firma Surfboard Holding B.V. betrieben. Die Suchmaschine speichert keine IP-Adressen und generiert keine Profile der Nutzer. Diese Meta-Suche fragt mehrere externe Suchmaschinen an, aber nicht Google. Ixquick.com wurde im Jan. 2009 mit dem Datenschutzsiegel EuroPriSe zertifiziert.

und
www.startpage.com wird ebenfalls von Surfboard Holding B.V. betrieben und ist mit dem Daten-

schutzsiegel EuroPriSe zertifiziert. Die Suchmaschine bietet privacy-freundlichen Zugriff auf die Google-Suche, ist also einen ideale Ergänzung zu Ixquick.com. Den Ixquick-Proxy zum anonymen Aufruf der Webseiten aus den Ergebnissen kann man mit Startpage auch nutzen.

Es handelt sich dabei um Metasuchmaschinen. Das bedeutet, sie bekommen von dir eine Anfrage und leiten diese dann an andere Suchmaschinen weiter. Die „besten“ Ergebnisse werden gesammelt und dir dann letztlich angezeigt. An wie viele Suchmaschinen eine Metasuchmaschine die besagte Anfrage weiterleitet, ist von Metasuchmaschine zu Metasuchmaschine anders. Zu Ixquick findet man Angaben zwischen 11 und 16 Suchmaschinen oder -portalen.

Neben diesem Punkt speichern Ixquick und Startpage keinerlei Daten von dir. Auch deine IP wird sofort wieder gelöscht und nicht mehr, wie es früher war, erst nach 48 Stunden. Die Suchmaschinen sind auch über SSL abrufbar und stehen in Sachen Suchergebnissen Google in nichts nach.

Als kleines Schmankerl bietet Ixquick die Möglichkeit, aus den Suchergebnissen heraus die Weltnetzseiten über einen anonymisierenden Proxy aufzurufen. Die aufgerufene Seite sieht damit nur eine IP-Adresse von Ixquick. Neben den Ergebnissen findet man einen kleinen Link „Proxy“.

Aus Sicherheitsgründen entfernt der Proxy JavaScript Code aus den aufgerufenen Weltnetzseiten. Es ist daher möglich, dass einige Seiten nicht wie erwartet funktionieren. Außerdem ist keine Eingabe von Daten in Textfeldern der aufgerufenen Weltnetzseiten möglich. Der Proxy kann die Seiten nur darstellen! Alternative Suchmaschinen in den Netzbetrachter integrieren

Mehr Datenschutz bedeutet nicht immer weniger Komfort. Ixquick kann mit sehr wenig Aufwand als Standardsuche in deinen Netzbetrachter integriert werden.

Bei Bedarf danach lässt sich jederzeit auch wieder mit einem Klick auf die vorherige Suchmaschine wechseln und umgekehrt, so dass bisherige Sucheinstellungen nicht ersetzt, sondern um weitere Auswahlmöglichkeiten ergänzt werden.

Das entsprechende Plugin findest du unter https://www.ixquick.de/deu/download-ixquick-plugin.html.

Wähle die dabei angebotene Konfiguration „HTTPS“, um die Übertragung der Suchanfragen und Suchergebnisse von und zur Ixquick Suchmaschine zu verschlüsseln und ein sonst an verschiedenen Stellen sehr einfaches Abhören und Protokollieren deiner Suchanfragen zu erschweren.

Wer nicht nur aus guten Gründen Google misstraut, sondern auch den Betreibern und den Datenschutzversprechen von Ixquick nicht gänzlich vertrauen mag, kann Ixquick im Gegensatz zu Google problemlos auch völlig anonym über den Anonymisierungsdienst Tor nutzen.

Für alle alternativen Suchmaschinen gilt, dass sie eine andere Sicht auf das Weltnetz bieten und die Ergebnisse sich von Google unterscheiden. Man sollte bei der Beurteilung der Ergebnisse beachten, dass auch Google nicht die reine Wahrheit bieten kann, sondern nur eine bestimmte Sicht auf das Weltnetz.

Letztlich bleibt es aber dir selbst überlassen, welche Suchmaschine du verwendest. Wir hoffen aber dich mit diesem Artikel in die richtige Richtung geschubst zu haben. Für dein Smartphone gibt es die App DuckDuckGo um anonym im Weltnetz zu suchen.

8.108 Versand von eBriefen

Obwohl Behörden durch Postüberwachung auch an Inhalte von Briefen kommen können, lässt du deswegen noch lange nicht deinen Briefkastenschlüssel auf der Strasse liegen. Gleiches sollte für

eBriefe gelten:

Mittlerweile gehen namhafte Weltnetz-Dienstleister von rund 30 Millionen eBriefen pro Tag aus, Spam ausgenommen. Trotz dieses erheblichen Umfangs wird nach wie vor in ebenso großem Umfang überwacht und mitgelesen.

Neben den besonderen Gefahren, denen wir als Systemgegner ausgesetzt sind, sollte schon allein der Gedanke der geschützten Privatsphäre einen Anstoß zum Verschlüsseln der eigenen eBriefe geben. Neben dem eigentlichen Unkenntlich machen der Nachrichten sollte man diese ebenfalls in regelmäßigen Abständen durchsehen und Altes & Erledigtes aussortieren.

Bestimmt möchtest du trotzdem nicht, dass zusätzlich auch noch Mitreisende, Hotelgäste oder andere Personen in der Nähe sehr leicht deine kompletten eBrief-Zugangsdaten inkl. Benutzername und Passwort sowie alle unverschlüsselten eBriefe mitlesen können, weil du diese z.B. im Cafe, auf Reisen oder im Hotel über das gleiche Netzwerk oder WLAN abrufen oder versenden. Genauso wie du beim sog. „Online-Banking“ oder beim Zugriff auf sog. „soziale Netzwerke“ verschlüsselte Verbindungen über HTTPS nutzt (Das eingeblendete Schloss-Symbol neben der Adressleiste), solltest du auch deine eBriefe nur über eine verschlüsselte Verbindung per POP3/SSL bzw. IMAP/SSL abholen sowie ausschliesslich über SMTP/SSL bzw. SMTP mit TLS versenden.

Dadurch schützt man nicht nur sich sondern auch die Personen zu denen man Kontakt aufgenommen hatte.

8.108.1 Anonyme eBrief Accounts

Das Nachdenken über die eBrief Kommunikation beginnt mit der Auswahl eines geeigneten eBrief Providers. Man braucht eine oder mehrere eBrief Adressen. Es ist empfehlenswert, für unterschiedliche Anwendungen auch verschiedene eBrief Adressen zu verwenden. Es erschwert die Profilbildung anhand der eBrief Adresse und verringert die Spam-Belästigung. Wenn Amazon, Ebay oder andere kommerzielle Anbieter zu aufdringlich werden, wird die mit Spam überschwemmte eBrief Adresse einfach gelöscht ohne die private Kommunikation zu stören.

Neben einer sehr privaten eBrief Adresse für Freunde könnte man weitere eBrief Adressen für Einkäufe im Weltnetz nutzen oder für politische Aktivitäten. Um nicht ständig viele eBrief Accounts abfragen zu müssen, kann man die für Einkäufe im Weltnetz genutzte eBrief Accounts auch an die private Hauptadresse weiterleiten lassen. Alle eBrief-Provider bieten diese Option bei einigen eBriefen.

Als eBrief Provider kann man einen zuverlässigen Anbieter im Weltnetz nehmen.

Außerdem bieten I2P und Tor spezielle Lösungen:

Das Invisible Internet Project (I2P) bietet mit Susimail einen anonymen eBrief-Service inclusive SMTP- und POP3-Zugang und Gateway ins Web oder mit I2P Bote einen serverlosen, verschlüsselten eBriefdienst.

TorMail gibt es als Hidden Service unter http://jhiwjjlqpyawmpjx.onion mit POP3 und SMTP Service. eBriefe werden auch aus dem normalen Web unter Adressen xxx@tormail.net angenommen.

Tor Privat Messaging unter http://4eiruntyxxbgfv7o.onion/pm ist ein Tor Hidden Service im Tor Onionland, um Textnachrichten unbeobachtet auszutauschen. Der Dienst kann nur im Webinterface genutzt werden.

Informationen über Langzeit-Kommunikationspartner können dazu verwendet werden, deinen Account zu deanonymisieren. Anhand der Freunde in der eBrief Kommunikation sind Schlussfolgerungen auf deine reale Identität möglich. **Wenn du einen wirklich anonymen eBrief Account für eine bestimmte Aufgabe benötigst - z.B. für Whistleblowing - dann musst du einen neuen Account erstellen. Lösche den Account, sobald du ihn nicht mehr benötigst und verwende ihn nicht für eBriefe an Bekannte und Freunde.**

8.108.2 Private Messages in Foren nutzen

Viele Diskussionsforen im Weltnetz bieten die Möglichkeit, private Nachrichten zwischen den Mitgliedern zu verschicken. Die Nachrichten werden in der Datenbank des Forums gespeichert und nicht per eBrief durch das Netz geschickt. Eine böse Gruppe ganz gemeiner Terroristen könnte sich also in einem Forum anmelden, dessen Inhalt sie überhaupt nicht interessiert. Dort tauschen sie die Nachrichten per PM (Private Message) aus und keiner bemerkt die Kommunikation. Es ist vorteilhaft, wenn das Forum komplett via HTTPS nutzbar ist und nicht nur beim Login HTTPS anbietet.

Die Nachrichten kann man mit OpenPGP verschlüsseln, damit der Administrator des Forums nichts mitlesen kann. Die Verwendung von Anonymisierungsdiensten sichert die Anonymität.

8.108.3 Mixmaster-Remailer

Der Versand einer Nachricht über Remailer-Kaskaden ist mit der Versendung eines Briefes vergleichbar, der in mehreren Umschlägen steckt. Jeder Empfänger innerhalb der Kaskade öffnet einen Umschlag und sendet den darin enthaltenen Brief ohne Hinweise auf den vorherigen Absender weiter. Der letzte Remailer der Kaskade liefert den Brief an den Empfänger aus.

Technisch realisiert wird dieses Prinzip mittels asymmetrischer Verschlüsselung. Der Absender wählt aus der Liste der verfügbaren weltweit verteilten Remailer n verschiedene Rechner aus, verschlüsselt der eBrief mehrfach mit den öffentlichen Schlüsseln der Remailer in der Folge ihres Durchlaufes und sendet das Ergebnis an den ersten Rechner der Kaskade. Dieser entschlüsselt mit seinem geheimen Schlüssel den ersten Umschlag, entnimmt dem Ergebnis die Adresse des folgenden Rechners und sendet die jetzt (n-1)-fach verschlüsselten eBrief an diesen Rechner. Der letzte Remailer der Kaskade sendet den Brief an den Empfänger.

Mitlesende Dritte können lediglich protokollieren, dass der Empfänger einen eBrief unbekannter Herkunft und evtl. unbekannten Inhaltes (verschlüsselt mit OpenPGP oder S/MIME) erhalten hat. Es ist ebenfalls möglich, Beiträge für News-Groups anonym zu posten.

Um die Traffic-Analyse zu erschweren, wird die Weiterleitung jedes eBriefs innerhalb der Kaskade verzögert. Es kann somit 2 - 12 Stunden dauern, ehe der eBrief zugestellt wird! Sollte der letzte Remailer der Kette die Nachricht nicht zustellen können (z.B. aufgrund eines Schreibfehlers in der Adresse), erhält der Absender keine Fehlermeldung. Der Absender ist ja nicht bekannt. Bei großen eBrief Providern werden die anonymen eBriefe aus dem Mixmaster Netzwerk häufig als Spam einsortiert. Es ist somit nicht sichergestellt, dass der Empfänger den eBrief wirklich zur Kenntnis nimmt! WICHTIG: Da der eBrief keine Angaben über den Absender enthält, funktioniert der Button „Antworten“ der Mail-Clients auf der Empfängerseite nicht sinnvoll! Die Antwort-Mail geht dann an den letzten Remailer der Kette, der sie in die Tonne wirft. Der Text des eBriefes sollte einen entsprechenden Hinweis enthalten!

Software zur Versendung anonymer eBriefe via Mixmaster:

Für Windows gibt es Quicksilver Für Linux gibt es „mixmaster“. Das Paket ist in allen Distributionen enthalten. Wer sich nicht mit der komplizierten Konfiguration beschäftigen möchte, der

kann eine Live-CD nutzen. Die JonDo Live-CD enthält mixmaster. Eine Anleitung zum Senden eines anonymen eBrief findet man in der Online-Hilfe zur Live-CD.

8.108.4 Spam-Schutz

Die eBrief Adresse ist ein wichtiges Identitätsmerkmal. Datensammler wie Rapleaf verwenden sie als ein Hauptmerkmal für die Identifikation, um darauf aufbauend Profile zu erstellen. Stichproben im Internet Traffic weisen einen hohen Anteil von Suchanfragen nach Informationen zu den Inhabern von eBrief Adressen aus.

Man muss die eigene eBrief Adresse nicht bei jeder Gelegenheit im Web angeben, wenn irgendwo eine eBrief Adresse verlangt wird (bei der Registrierung in Foren, einfachen Blog Postings usw). Um die eigene eBrief Adresse nicht zu kompromittieren und trotzdem diese Angebote zu nutzen, kann man die folgenden „Fake“ eBriefadressen nutzen.

8.108.5 AnonBox des CCC (24-48h)

Bei der AnonBox.net kann ein eBrief Account für den Empfang von einer Nachricht erstellt werden. Der Account ist bis 24:00 Uhr des folgenden Tages gültig und nicht verlängerbar. Eingehende Nachrichten kann man nur im Webinterface lesen und sie werden nach dem Abrufen gelöscht. Sie können nur 1x gelesen werden! Zusammen mit dem eBrief wird auch der Account gelöscht. Man kann praktisch nur einen eBrief empfangen!

Beim Erzeugen einer eBrief Adresse erhält man einen Link, unter dem man ankommende eBriefe lesen kann. Wenn noch nichts angekommen ist, dann bleibt die Seite leer. Der Link ist als Lesezeichen zu speichern, wenn man später nochmal nachschauen möchte.

Die AnonBox bietet als einziger Anbieter SSL-Verschlüsselung und verwendet ein Zertifikat, das von CAcert.org signiert wurde. In den meisten Browsern ist diese CA nicht als vertrauenswürdig enthalten. Das Root-Zertifikat dieser CA muss von der Weltnetzseite zusätzlich importiert werden.

8.108.6 Wegwerf-eBrief-Adressen

Einige Anbieter von Wegwerf-eBrief-Adressen bieten einen sehr einfach nutzbaren Service, der keinerlei Anmeldung erfordert und auch kein Erstellen der Adresse vor der Nutzung. eBrief Adressen der Form „pittiplatsch@trash-mail.com“ oder „pittiplatsch@weg-werf-email.de“ kann man überall und ohne Vorbereitung unbekümmert angeben. Das Postfach ist unbegrenzt gültig.

In einem Webformular auf der Seite des Betreibers findet man später alle eingegangenen Spam- und sonstigen Nachrichten für das gewählte Pseudonym. Für das Webinterface des Postfachs gibt es in der Regel keinen Zugriffsschutz. Jeder, der das Pseudonym kennt, kann die Nachrichten lesen und löschen. Nachrichten werden nach 6-12h automatisch gelöscht. Das Firefox Add-On „Bloody Vikings“ vereinfacht die Nutzung von Wegwerf-eBrief-Adressen. Nach der Installation kann ein bevorzugter Dienst für die Wegwerfadressen gewählt werden. Damit kannst du deine eigene eBrief Adresse schützen, indem du auf weniger vertrauenswürdigeren Seiten nicht deine eigentliche eBrief Adresse eingibst.

Einiger Anbieter (natürlich unvollständig):

spambog.com (weitere eBrief Domains auf der Webseite, Account kann mit Passwort gesichert werden, Löschen der eBriefe ist möglich, Session-Cookies erforderlich)
OneWayMail.com (weitere eBrief Domains auf der Webseite, keine Cookies oder Javascript nötig, eBriefe können gelöscht werden, 5 weitere Domains)

trash-mail.com (keine Cookies oder Javascript nötig, eBriefe können gelöscht werden)
mailcatch.com (keine Cookies oder Javascript nötig, eBriefe können gelöscht werden)
mailinator.com (bietet 5 weitere Domains, keine Cookies oder Javascript nötig, eBriefe können gelöscht werden, POP3-Abruf möglich)
weg-werf-email.de (Session-Cookies erforderlich, Passwortschutz möglich)
GuerrillaMail (HTTPS, Session-Cookies erforderlich, eBriefe können gelöscht werden)

In der Regel speichern diese Anbieter die Informationen über eingehende eBriefe sowie Aufrufe des Webinterface und stellen die Informationen bei Bedarf den Behörden zur Verfügung. **(nur mit Anonymisierungsdiensten geeignet!)**

8.108.7 Temporäre eBrief Adressen

Im Gegensatz zu Wegwerf-eBrief-Adressen muss man eine temporäre eBrief Adresse zuerst auf der Webseiten des Anbieter erstellen, die dann für 10min bis zu mehreren Stunden gültig ist. Erst danach kann diese eBrief-Adresse verwendet werden. Bei Bedarf kann die Verfügbarkeit der eBrief Adresse mehrfach verlängert werden.

10minutemail.com (10min gültig, keine Cookies und kein JavaScript nötig)
Tempsky (15min gültig, Session-Cockies müssen freigegeben werden, gewünschte eBrief Adresse kann festgelegt werden)
Tempmailer.de (60min gültig, Session-Cockies müssen freigegeben werden)
freemail.ms (24h gültig, Session-Cockies müssen freigegeben werden)
emailisvalid.com (15min gültig, Session-Cookies und JavaScript freigeben)
edv.to (15min gültig, Session-Cookies freigeben)
tempemail.co.za (30min gültig, Session-Cookies freigeben)
Squizzy.de (60min gültig, Session-Cookies freigeben)
FakeInbox (60min gültig, Session-Cookies freigeben)
topranklist.de (6 Stunden gültig, Session-Cookies freigeben)
ieh-mail.de (24 Stunden gültig, Session-Cookies und JavaScript freigeben, HTTPS zum Abrufen der eBriefe, API für Anbindung eigener Anwendungen)

Um eine temporäre Adresse für die Anmeldung in einem Forum o.ä. zu nutzen, öffnet man als erstes eine der oben angegebenen Weltnetzseiten in einem neuen Browser-Tab. Session-Cookies sind für diese Seite freizugeben, mit JavaScript sind die Webseiten oft besser bedienbar.

Nachdem man eine neue temporäre eBrief-Adresse erstellt hat, überträgt man sie mit Copy & Paste in das Anmeldeformular uns schickt das Formular ab. Dann wechselt man wieder zu dem Browser-Tab der temporären eBrief Adresse und wartet auf den eingehenden Bestätigungs-eBrief. In der Regel einhält dieser eBrief einen Link zur Verifikation. Auf den Link klicken - fertig. Wenn der Browser-Tab mit der temporäre eBrief Adresse geschlossen wurde, hat man keine Möglichkeit mehr, ankommende eBriefe für diese Adresse zu lesen.

8.108.8 eBrief Provider abseits des Mainstream

Wenn eine eBrief Adresse nur für die Anmeldung in einem Forum oder das Veröffentlichen eines Kommentars in Blogs benötigt wird, kann man Temporäre eBrief Adressen nutzen. Es kostet Geld, einen zuverlässigen eBrief Service bereitzustellen. Es ist durchaus sinnvoll, die „alles kostenlos Mentalität“ für einen vertrauenswürdigen eBrief Provider fallen zu lassen.

Eine kleine Liste von eBrief Providern abseits des Mainstream:

protonmail.com (kostenfrei)
Posteo.de und aikQ.de (deutscher eBrief Provider, Accounts ab 1,- Euro pro Monat, anonyme

Accounts möglich mit Bezahlung per Brief)
neomailbox.com (anonymes eBrief Hosting in der Schweiz, Accounts ab 3,33 Dollar pro Monat, anonyme Bezahlung mit Pecunix oder Liberty Reserve möglich)
VFEmail (anonymer eBrief Provider, benötigt eine Wegwerf-Adresse für Registrierung, kostenfreie Accounts mit POP3/SMTP und beliebig vielen temporären eBrief Adressen, für Premium-Nutzer werden die IP-Adressen der Absender beim Senden maskiert.)
CryptoHeaven (Accounts ab 60 Dollar pro Jahr, einfache Verschlüsselung der Kommunikation mit Accounts beim gleichen Provider, Offshore registrierte Firma, Server in Kanada)
runbox.com (norwegischer eBrief Provider, Server stehen ebenfalls in Norwegen, Accounts ab 1,66 Dollar pro Monat)
Startmail.com Die niederländischen Firma Surfboard Holding B.V. betreibt bisher die privacy-zertifizierten Suchmaschinen Startpage.com und Ixquick.com.
Aufgrund des US PATRIOT Act (insbesondere S. 215ff) und der 4. Ergänzung des FISA Amendments Act ist es für US-Behörden ohne juristische Kontrolle möglich, die Kommunikation von Nicht-US-Bürgern zu beschnüffeln. Nach Ansicht der US-Behörden reicht es aus, wenn die Server in den USA stehen. In der EU-Studie Fighting cyber crime and protecting privacy in the cloud warnen die Autoren insbesondere vor politischer Überwachung. Deshalb können wir diesen folgenden eBrief Provider nur eingeschränkt empfehlen.

0x300.com (ein von Politischen Aktivisten betriebener eBrief Service)
Am 9. November 2007 beschloss der Bundestag mit den Stimmen von CDU, CSU und SPD die Vorratsspeicherung in Deutschland. Bundesbürger konnten also seit 1. Januar 2008 nicht mehr unbesorgt miteinander kommunizieren keine IP Speicherung und Server in den USA)

Informationen über Langzeit-Kommunikationspartner können dazu verwendet werden, deinen Account zu deanonymisieren. Anhand der Freunde in der eBrief Kommunikation sind Schlussfolgerungen auf deine reale Identität möglich. Wenn du einen wirklich anonymen eBrief Account für eine bestimmte Aufgabe benötigst - z.B. für Whistleblowing - dann musst du einen neuen Account erstellen. Lösche den Account, sobald du ihn nicht mehr benötigst und verwende ihn nicht für eBriefe an Bekannte und Freunde.

8.109 Vorratsdatenspeicherung und staatliche Überwachung

Ob du telefonierst, jemanden eine eBrief schickst oder eine Kurzmitteilung (SMS) versendest - jeder Schritt wurde protokolliert und sechs Monate lang gespeichert, damit Ermittlungsbehörden sie bei Bedarf abfragen können.

Erst im März 2010 kippte das Bundesverfassungsgericht das umstrittene Gesetz - vorerst. Was das für dich bedeutet und wie du dich zumindest ein kleines bisschen Privatheit bewahren können, haben wir auf diesen Seiten für dich zusammengestellt. Vorratsdatenspeicherung und staatliche Überwachung griffen und greifen massiv in die Bürgerrechte ein.

8.109.1 Diese Daten wurden gespeichert

Das Gesetz zur Vorratsdatenspeicherung schrieb vor, dass Weltnetz- und Telefon-Provider alle Daten speichern, die mit einer Verbindung zu tun haben - und zwar in jedem Fall sechs Monate lang. Seit Januar 2008 galt das für Telefongespräche im Festnetz und Mobilfunk, ein Jahr später trat die zweite Stufe in Kraft. Seitdem werden auch Internet- und eBriefdaten gespeichert.

Es ging dabei um folgende Daten:

Telefonate über Festnetz
Telefonanbieter mussten die Rufnummer des anrufenden und des angerufenen Anschlusses speichern. Außerdem wurden der Beginn und das Ende der Verbindung festgehalten

Telefonate über Mobilfunk
Deine Mobilfunknummer und die Mobilfunknummer deines Gesprächspartners. Zeitpunkt und Dauer der Verbindung. Funkzelle (=Ort), in der du dich während des Gesprächs aufgehalten hast. Funkzelle (=Ort), in der dein sich Gesprächspartner sich während des Gesprächs aufgehalten hat

IP-Telefonie
Beim Telefonieren über das Weltnetz wurden Zeitpunkt und Dauer der Verbindung, außerdem deine IP-Adresse und die IP-Adresse des Agerufenen protokolliert Über die IP-Adresse ist jeder einzelne Rechner im Weltnetz eindeutig identifizierbar

Versand von SMS
Deine Mobilfunknummer und die Nummer des Empfängers. Zeitpunkt des SMS-Versands und Zeitpunkt des SMS-Empfangs. Funkzelle (=Ort), in der du dich zum Zeitpunkt des SMS-Versands befandest Versand von Fax

Die Rufnummer des Absenders der Fax-Botschaft, die Rufnummer des Empfängers, Zeitpunkt und Dauer der Verbindung
Versand von eBriefen
Alle Anbieter von eBrief-Diensten mussten bestimmte Daten ihrer Kunden festhalten. Bei Versand eines eBriefes - die Kennung deines elektronischen Postfachs und deine IP-Adresse sowie die Kennung des elektronischen Postfachs jedes Empfängers deiner Nachricht. Beim Empfang eines eBriefes die Kennung des Postfachs des Absenders und des Empfängers der Nachricht sowie die IP-Adresse des Absenders. Wenn du auf ein Postfach zugreifst, die Kennung des Fachs und deine IP-Adresse Verbindungen ins Weltnetz
Gespeichert werden alle Daten, die beim Surfen im Weltnetz anfallen. Das sind Online-Zugangsdaten wie die IP-Adresse und die Anschlusskennung (Rufnummer oder DSL-Kennung). Außerdem werden der Beginn und das Ende der Nutzung festgehalten.

8.109.2 Wer speichert die Verbindungsdaten - und wie lange?

Die Vorratsdatenspeicherung sah vor, dass die Datenberge von den Telefongesellschaften, den Internet-Providern und den Anbietern öffentlich zugänglicher Internetzugänge (etwa HotSpots in Flughäfen und Bahnhöfen) gespeichert werden. Und das auf eine Dauer von sechs Monaten. Anschließend müssen die Daten binnen einer Frist von einem Monat gelöscht werden.

Wer durfte die gespeicherten Verbindungsdaten einsehen?

Polizeidienststellen
Staatsanwaltschaften
Verfassungsschutzämter
Bundesnachrichtendienst
Militärischer Abschirmdienst

8.109.3 Welche Bestandsdaten werden gespeichert?

Anbieter von Festnetz-Telefonie, Mobilfunk (Handy) oder Internet-Telefonie haben unabhängig von der Vorratsdatenspeicherung folgende Bestandsdaten ihrer Kunden abzufragen und zu speichern:

Rufnummern bzw. Mailadresse
Name des Kunden
Anschrift des Kunden

Geburtsdatum des Kunden
Datum des Vertragsbeginns
ggf. Anschrift des Festnetzanschlusses

Zudem sind die Anbieter verpflichtet, auf Anfrage spezielle Daten ihrer Kunden herauszugeben. Dazu gehören unter anderem:

dynamische (also von Fall zu Fall vergebene) IP-Adressen
Passworte
PIN und PUK

8.109.4 Ist das letzte Wort schon gesprochen?

Im März 2010 erklärte das Bundesverfassungsgericht die Vorratsdatenspeicherung in ihrer bis dahin geltenden Form für verfassungswidrig und nichtig. Alle bis dahin gespeicherten Daten müssten sofort gelöscht werden, so die Karlsruher Richter.

Ein grundsätzliches Verbot der Vorratsdatenspeicherung gab es allerdings nicht. Die Richter stellten nur fest, dass eine solche Massen-Speicherung nach klareren und verfassungsrechtlich korrekten Regeln erfolgen müsse. Die Bundesregierung kündigte folglich ein neues Gesetz an.

Januar 2015
Es war abzusehen, dass nach den islamistischen Anschlägen in Paris die Stimmen hierzulande wieder laut werden und eine Vorratsdatenspeicherung (VDS) fordern. Bundeskanzlerin Angela Merkel (CDU) und die Sicherheitsbehörden drängen vehement auf die Vorratsdatenspeicherung. Sie diene der Sicherheit und Täter sowie Mittäter können besser erkannt werden. Auch könne man damit besser ein Anschlag verhindern, wenn man vorab schon wüsste, wer mit wem und wie Kontakt hält.

Der Arbeitskreis Vorratsdatenspeicherung informiert laufend über die aktuelle Entwicklung.

9 Mobiltelefon

Datenspuren auf deinem Mobiltelefon

Mobiltelefone und sogenante „Smartphones“ sind in puncto Sicherheit ähnlich wie Computer und Laptops zu behandeln. Dies umfasst optimalerweise die Einrichtung eines Virenscanners auf dem Mobiltelefon und die Installation von Betriebssystem-Updates. Außerdem sollten sensible Zugangsdaten wie für die mobile Nutzung von Bankdiensten nicht auf dem Gerät gespeichert werden. PINs bzw. Passwörter nutzen

Beim Anschalten eines Handys wird standardmäßig die Persönliche Identifikationsnummer (PIN) der SIM-Karte abgefragt. Auch wenn es bequemer ist: Diese Funktion sollte nicht deaktiviert werden. Zusätzlich lässt sich bei vielen Mobiltelefonen eine Geräte-PIN einrichten. Diese Geräte-PIN stellt sicher, dass ein gestohlenes Mobiltelefon nicht von einem Unbefugten mit einer anderen SIM-Karte genutzt werden kann. Dadurch lässt sich der Zugriff auf die gespeicherten persönlichen Kontaktdaten, Nachrichten, Passwörter etc. wirkungsvoll verhindern.

Datenverbindungen deaktivieren
Verbindungen für den Datenaustausch etwa über Bluetooth oder WLAN sind eine potenzielle Sicherheitslücke. Sie sind ein mögliches Einfallstor für Viren und Trojaner, die persönliche Daten ausspähen können. Werden die Datenverbindungen nicht verwendet, sollte man sie deshalb deaktivieren.

Zusatzprogramme sorgfältig prüfen
Smartphone-Nutzer sollten aufmerksam prüfen, welche mobilen Zusatzprogramme oder „Apps“ sie installieren und verwenden. Bei einigen „Apps“ werden vom Anbieter personen- und ortsgebundene Daten gesammelt und verarbeitet. Darüber hinaus besteht das Risiko, dass Schadsoftware getarnt als „App“ auf einem Mobilgerät installiert wird. So gab es bislang mehrere Fälle von manipulierten „Apps“, die beispielsweise Kontodaten des mobilen Bankings ausspähen können. Einen Anhaltspunkt für die Vertrauenswürdigkeit einer „App“ bieten die Bewertungen anderer Anwender - im Zweifel sollte auf die Installation eines Zusatzprogramms verzichtet werden.

Wenn das Telefon verloren geht
Über eine Kennziffer, die so genannte IMEI, lässt sich jedes Mobiltelefon zweifelsfrei identifizieren. Sollte ein Gerät nach Verlust oder Diebstahl gefunden beziehungsweise sichergestellt werden, kann geprüft werden, ob ein Telefon mit der entsprechenden Nummer als verloren gemeldet wurde. So lässt sich der Besitzer bestimmen, sofern dieser seine Gerätenummer für den Notfall notiert hat. Die Kennziffer findet sich auf fast jedem Telefongehäuse, meist unter dem Akku oder auf dem SIM-Kartenhalter.

9.1 Demotipps für den sicheren Umgang mit Mobiltelefonen

Seit einigen Jahren erfahren wir immer mehr, zu welchen Mitteln Sicherheitsbehörden greifen, um Kommunikationen von Demonstranten flächendeckend zu überwachen. Gleichzeitig sollte aber das Mithören unserer privaten Telefonate und die Durchsuchung unserer mobilen Geräte nicht ohne Anordnung möglich sein. Und es geht auch nicht nur um Inhalte: Schon die Tatsache, an einer bestimmten Demo teilgenommen zu haben, kann eine erhebliche Aussagekraft haben.

Eine Demo ist natürlich ein historisches Ereignis, das man festhalten möchte. Man will Infos, Fotos und Videos sofort mit Freunden oder auch der ganzen Welt teilen. Daher nehmen wir unsere mobilen Geräte mit und sehen uns dann mit dem Problem konfrontiert, dass wir auf eben jenen Geräten auch eine Menge private Daten gespeichert haben. Wir hoffen, dass wir euch daher mit dieser Anleitung einige Fragen beantworten und euch Tipps geben können, wie man seine Daten am besten sichert und welche Rechte ihr während der Demo habt, sollte es einmal brenzlig werden. Generell gilt natürlich: Seid kreativ, Humor ist stärker als Gewalt!

Niemand und kein Gerät ist jemals 100% sicher, aber es gibt ein paar Dinge, die ihr für die Sicherheit eurer persönlichen Daten tun könnt, bevor ihr auf die Straße geht. Dieser Leitfaden, der an einen Guide der EFF angelehnt ist, gibt euch einige gute Tipps.

9.2 Vor der Demo

Mach dir Gedanken darüber, welche Daten sich auf deinem Telefonen befinden. Zwar gibt es einige rechtliche Hürden, ehe jemand dein Mobiltelefon beschlagnahmen und durchsuchen darf, doch ist es alles andere als sicher, dass euch das im Ernstfall wirklich hilft.

Und auch wenn niemand euer Gerät in die Hände bekommt, drohen durchaus Gefahren für die Privatsphäre. Denn seit 2012 ist bekannt, dass die Polizei flächendeckende Funkzellenabfragen während Demos durchführt. Bei einer Funkzellenabfrage werden alle Verbindungsdaten ausgewertet, die in einer bestimmten, räumlich bezeichneten Funkzelle in einem bestimmten Zeitraum angefallen ist. Die Berliner Polizei hat beispielsweise im letzten Jahr auf diese Weise 50 Millionen Verkehrsdatensätze gesammelt. Damit lässt sich quasi ein elektronisches Register anlegen, wer an welcher Demo teilgenommen hat - und zwar auch ohne dass es den geringsten Verdacht gegen die Personen gäbe, die so ins Raster der Behörden geraten. Gegen die Funkzellenabfrage ist leider kaum ein Kraut gewachsen, sofern man das Mobiltelefon nicht in den Flugzeug-Modus

stellen will. Aber was die Inhalte des Mobiltelefon angeht haben wir eine Reihe von Empfehlungen:

Schütze deine Daten! Wenn du noch irgendwo ein älteres Mobiltelefon hast, ist es empfehlenswert, dein jetziges vorübergehend zu ersetzen. So kannst du für den Fall der Fälle sicher gehen, dass deine Fotos, dein Adressbuch und andere Daten sicher zu Hause liegen.

Mach ein Back-up. Eine weitere und einfache Möglichkeit ist es, vor der Demo ein Back-up aller Inhalte, deines Adressbuchs und aller Nachrichten zu machen, um dann dein Gerät komplett löschen zu können. Dieses leere Gerät kannst du dann problemlos mit zur Demo nehmen. Nach der Demo holst du dir einfach alles mit dem Back-up zu Hause zurück. Wenn du allerdings meinst, dass du gar kein Mobiltelefon brauchst, bringe einfach keins mit.

Sperre dein Mobiltelefon mit einem Passwort. Der Passwortschutz kann dein Mobiltelefon vor physischen Durchsuchungen schützen - aber vergiss nicht, dass er von Geheimdiensten oder anderen Behörden eventuell umgangen werden kann. Eine Kombination aus Zahlen und Buchstaben ist generell sicherer, denn eine Zahlenkombination lässt sich in wenigen Minuten knacken. Weitere Informationen zum Thema Passwort: Passwortschutz

Benutze verschlüsselte Kommunikationswege. SMS können generell von deinem Anbieter gespeichert und mitgelesen werden - oder auch mit Hilfe von diversem Überwachungsmaterial, das in der Nähe der Demo aufgestellt wird (Stichwort IMSI-Catcher). Du solltest dich mit deinen Freunden vor der Demo mit verschiedenen Verschlüsselungstechniken und -diensten vertraut machen, um deine Nachrichten vor fremdem Zugriff zu schützen. Direkte Nachrichten über soziale Netzwerke können beim Senden teilweise verschlüsselt werden. Strafverfolgungsbehörden haben aber die Möglichkeit, mit Hilfe von Anordnungen die Herausgabe der Daten bei den Unternehmen anzufordern.

Eine gute Möglichkeit für den besseren Schutz von Nachrichten ist die sogenannte Ende-zu-Ende-Verschlüsselung. Mit Apps wie TextSecure (Whisper Systems) kannst du deine SMS und mit ChatSecure (Guardian Project) dein Instant-Messaging verschlüsseln. Auch die mobile Version von Cryptocat ist ganz gut für verschlüsselte Chats.

In Deutschland relativ verbreitet ist außerdem die (kostenpflichtige) App Threema. Leider ist die Software nicht OpenSource, aber sicherlich doch etwas sicherer als offene Kommunikation über Facebook oder SMS.

Wichtig: Ende-zu-Ende-Verschlüsselung schützt nicht deine Metadaten. Mit anderen Worten: Selbst wenn du alles verschlüsselst, können Behörden je nach System evtl. weiterhin sehen, mit wem du wann und wie lange telefonierst oder Nachrichten austauschst.

9.3 Auf der Demo

Behalte die Kontrolle über dein Telefon. Es ist empfehlenswert, dein Mobiltelefon immer bei dir zu tragen und es nur dann einer Person deines Vertrauens in die Hand zu geben, wenn du meinst, dass dir eine Verhaftung bevorsteht. In jedem Fall solltest du dein Mobiltelefon so einstellen, dass sich der Bildschirm sehr schnell automatisch sperrt. Es gibt keine rechtliche Verpflichtung, irgendwelchen Beamten seine Passwörter zu verraten. Das sollte man daher auch nicht tun!

Mache Bilder und Videos von der Demo. Wir haben alle das Recht darauf, alles aufzunehmen, was sich vor unseren Augen im öffentlichen Raum abspielt. Obwohl die Polizei das nicht so gerne sieht und sich hin und wieder dagegen wehrt, meint das Bundesverfassungsgericht, dass „Dokumentationen von Polizeieinsätzen im öffentlichen Interesse“ liegen. Lese dir zur Sicherheit vor der Demo

die Sicherheitshinweise hier auch noch einmal genau durch.

Außerdem könnte man erwägen, Dienste zu nutzen, die das gesammelte Material direkt auf einen Server hochladen. Streamingdienste und sogar soziale Netzwerke sind praktisch, um zu verhindern, dass Beamte sie von den Geräten löschen können.

Nutzt Tor oder VPNs. Wenn du etwas im Netz nachschauen und surfen willst, kannst du dies anonym über das Tor-Netzwerk tun. Für Android und iOS gibt es beispielsweise Orbot und Orweb. Eine weitere Alternative ist die Nutzung von bezahlten VPN-Diensten (die den Zugriff auf das Weltnetz durch Tunnel ermöglichen), die zwar schneller als das Tor-Netzwerk sind, aber weniger gut deine Identität schützen.

Schminkt euch! Es gibt überall Kameras, die alle Demoteilnehmer die ganze Zeit filmen. Ohne es zu wissen, kann dein Bild also schnell in einer Datenbank landen.

9.4 Hilfe, ich werde verhaftet

Du hast das Recht zu schweigen - Das betrifft auch Informationen zu deinem Telefon. Bleibe immer ruhig und freundlich. Auf Verlangen sollte man sich zwar mit einem Personalausweis ausweisen und Angaben zur Person machen können - darüber hinaus darf man sich aber gegen jede weitere Mitarbeit sträuben. Du kannst eine Durchsuchung höflich verweigern und erklären, alle weiteren Fragen nicht ohne die Gegenwart eines Anwalts zu beantworten. Wenn ein Polizeibeamter dein Telefon sehen möchte, sag ihm freundlich und bestimmt, dass du einer Durchsuchung deines Geräts nicht zustimmst. Sollte der Beamte nach deinem Passwort fragen, verweigere die Auskunft und fordere einen Anwalt. Jede Verhaftung verläuft anders und du solltest dich von einen Anwalt beraten lassen, damit du in dieser speziellen Situation Unterstützung bekommst.

Bitte beachte, dass die Polizei dich vielleicht nicht zur Herausgabe deiner Passwörter überreden kann - sie kann aber alles dafür tun, um dich unter Druck zu setzen. Sie können dich zeitweise festhalten, wenn du die Kooperation verweigerst. Du hast aber das Recht, spätestens am folgenden Tag einem Richter vorgeführt zu werden. Einfach wegsperren können sie dich also nicht.

Oft werden bei Demonstrationen auch Nummern von Anwälten, die während der Demo angerufen werden können, verteilt. Zudem steht oft eine ËA-Nummerßur Verfügung, die du anrufen solltest, wenn du siehst, dass ein Freund von dir verhaftet wird. Die Leute kümmern sich dann um alles weitere und versuchen, die betroffene Person schnellstmöglich wieder frei zu bekommen.

9.5 Nützliche Informationen zu deinem Mobiltelefon

Das von Traditionsdogmatikern unter Nationalisten lange Zeit verteufelte Mobiltelefon (Handy) hat mittlerweile überall Einzug gehalten, es ist für nahezu jeden Aktivisten zum unverzichtbaren Bestandteil der Kommunikation geworden. Oft mischen sich der private, persönliche Gebrauch mit politischen Kontakten. Das ist praktisch und eröffnet viele neue Möglichkeiten, etwa bei Demonstrationen, politische Aktionen zu koordinieren. Na und um die soll es an dieser Stelle gehen.

Wir wollen dabei nicht grundsätzlich über die Zwiespältigkeit der Technik diskutieren. In erster Linie wollen wir einen Praxis-Leitfaden an die Hand geben, der dich im Umgang mit Mobiltelefonen sensibilisieren und dir aufzeigen soll, was die dunkle Seite der Technik mittlerweile alles kann. Die Überwachung von Telefonen ist für die Polizei zum meisten genutzten Repressionsmittel überhaupt geworden. Es ermöglicht (mit einer richterlichen Anordnung) Gespräche zu belauschen, und versetzt die Polizei auch in die Lage, dich zu lokalisieren, wenn du ein eingeschaltetes Mobiltelefon dabei hast.

Zum Standardprogramm bei Festnahmen gehört klar auch die Auswertung deiner eingespeicherten Nummern, die ein mehr oder weniger vollständiges Kontaktbild deines Umfeldes liefern. Damit ist das Mobiltelefon für den staatlichen Repressionsapparat viel interessanter, als es früher ein normales Telefon in einer Wohnung war. In der Bewegung werden die Gefahren, die von der unbedachten Benutzung von Mobiltelefonen ausgehen, unserer Meinung nach deutlich unterschätzt. Viele Aktivisten sprechen beispielsweise grundsätzlich kein Wort über kleinste Fragen in den eigenen vier Wänden (was sicherlich sinnvoll ist!). Dabei wird der große Lauschangriff, also das Verwanzen von Wohnungen, jedes Jahr nur ein paar Mal angewandt, (meistens bei Mordermittlungen und bei Drogenprozessen oder Ähnliches). **Telefone wurden 2005 dagegen in fast 49.230 Fällen abgehört, die Ortung über Mobiltelefone dabei nicht mitgezählt. Fast alle abgehörten Telefone waren Mobiltelefone.**

Das Telefon ist also das Einfallstor Nummer 1, um Erkenntnisse über Kontakte, Aufenthaltsorte und Gespräche von Aktivisten zu erhalten. Das solltest du dir immer bewusst machen.

Wir unterstellen dabei, dass du nichts am Telefon selbst besprichst, was irgendwelche politischen Referenzen hat - dass sensible politische Sachen nichts am Telefon zu suchen haben, ist ja wohl eh klar! Prinzipiell ist es auch möglich, bei Telefonen über die Software das Mikrofon unbemerkt zu aktivieren und damit unbemerkt Gespräche zu lauschen. Ebenso kann eine Hardwaremanipulation nach längeren nicht Auffindens des Mobiltelefons sowie beim Kauf über dubiosen Quellen (z.B. Onlineauktionen) nicht ausgeschlossen werden. Allerdings spielen diese Methoden in der Praxis nach unserem Wissen keine große Rolle. Dennoch solltest du dein Mobiltelefon nicht angeschaltet lassen, und vorsichtshalber den Akku entfernen, wenn du sensible Gespräche führst.

9.6 Wie funktioniert das Mobiltelefon?

Grundsätzlich hinterlässt dein Mobiltelefon bei der Benutzung zwei digitale „Fingerabdrücke“: Die IMSI- und die IMEI Nummer.

Die IMSI-Nummer
(IMSI steht für International Mobile Subscriber Identiy) ist der individuelle Code deiner SIM-Karte, die meist 15-stellig ist. Mit der IMSI-Kennung lässt sich anhand der ersten 3 Ziffern feststellen, aus welchem Land deine Karte ist. Die nächsten beiden Zahlen sagen, welche Mobilfunkfirma deine Karte ausgegeben hat (T-Mobile, Vodafone, E-Plus, ...). Danach kommt eine individuelle Seriennummer. Der Verkaufsweg der IMSI-Nummer ist relativ simpel über die Register der Mobilfunkfirmen nachvollziehbar. Die IMSI wird bei jedem Gespräch übermittelt.
Die IMEI-Nummer
(IMEI steht für International Mobil Equipment Identity) ist immer 15-stellig und findet sich innen im Gerät. Sie identifiziert dein individuelles Telefon. Anhand der IMEI lässt sich auch zurückverfolgen, aus welchem Land dein Telefon stammt. Die ersten beiden Stellen geben Aufschluss über das Land, deutsche IMEIs beginnen dann mit 49. Die drei Zahlen, die dann kommen, bezeichnen den Hersteller (also Siemens, Nokia, ...). Die nächsten beiden Ziffern sagen, in welchem Land das Gerät produziert wurde. Erst dann kommt die aktuelle Seriennummer. Der Verkaufsweg der IMEI-Nummer ist nachvollziehbar, was aber für die Polizei zeitaufwendig und mühselig ist. Auch die IMEI wird bei Nutzung des Telefons übermittelt.

Wenn du also in deinem Gerät die Karte wechselst, benutzt du eine neue IMSI, aber weiter die alte IMEI. Wegen des mehr werdenden Diebstahls von Mobiltelefonen haben die Mobilfunkhersteller auf Druck des Staates in England mittlerweile ein zentrales IMEI-Register angelegt, in dem sämtliche Geräte mit ihrer IMEI registriert sind. Das Ziel ist, bei Diebstahl nicht nur die Karte (also die IMSI-Nummer) sperren zu können, sonder auch das Gerät selbst (über die IMEI). Damit würde ein gestohlenes Mobiltelefon wertlos - ganz nebenbei eröffnen sich aber auch neue Überwachungsmöglichkeiten, weil die Identifizierung eines Gerätes, des Kaufortes und -datums usw. sehr

unproblematisch wird.

In der BRD ist die Polizei noch nicht so weit, nach unserem letzten Stand hat allerdings Vodafone freiwillig mit dem Aufbau eines solchen Registers begonnen. Übrigens gibt es auch dagegen Gegenmittel: Im Weltnetz gibt es Programme, mit denen sich elektronisch die IMEI eines Programmes manipulieren lässt. Weil das auch die Bullen wissen, steht die Manipulation der Gerätenummer in England mittlerweile unter Strafe. Soweit unser kleiner Ausflug in die Welt der IMEI. Prinzipiell funktionieren Mobiltelefone so:

Wenn du dein Gerät einschaltest, meldet es sich im Telefonnetz mit seiner IMSI-Nummer und der IMEI an, wobei für die Firmen nur die IMSI wichtig ist. Der Mobilfunkbetreiber, bei dem du dich eingeloggt hast (also beispielsweise E-Plus) registriert deine Daten in einem Besucherregister und fragt anschließend bei deiner Mobilfunkfirma nach, ob deine Daten korrekt sind. Anschließend ist deine Anmeldung gespeichert und du darfst telefonieren.

Allerdings ist damit noch nicht dein Aufenthaltsort bekannt - jedenfalls nicht genau. Die Mobilfunknetze sind nach dem Schachtelprinzip aufgebaut: Die kleinste Einheit sind die Antennen, die meinst auf Dächern aufgebaut sind. Um die Antennen verwalten zu können, sind mehrere Antennen zu einer größeren Einheit zusammengefasst, der sogenannten BSS (Base Station Subsystem). Mehrere dieser BSS ergeben wiederum eine Local Area, kurz LA genannt.

Was wie technisch uninteressantes Kauderwelsch klingt, hat praktische Folgen. Denn die Mobilfunkfirmen wissen nicht automatisch, wo du dich befindest. Angemeldet bist du erst einmal nur in einer Local Area, die je nach Netzabdeckung ganz schön groß sein kann - bis zu einigen Hundert Quadratkilometern. Auf diese Weise reduzieren die Mobilfunkfirmen die Datenmengen. Es ist ja schließlich nicht entscheidend, mehr über dich zu wissen, als dass du dich in der oder dieser Region eingeloggt hast. Auch, wenn ein Mobiltelefon innerhalb einer Local Area den Ort wechselt, ohne dass das Telefon benutzt wird, findet ein Update in der Regel nicht statt. Erst, wenn du dein Mobiltelefon aktiv benutzt, wird präzise der genaue Standort gespeichert (also von welcher Antenne aus welcher BSS, dein Signal kommt). Das Gleiche geschieht nach einer längeren Phase der Inaktivität (zwischen einer halben Stunde und mehreren Stunden).

Die Ortung von Mobiltelefonen schwankt also zwischen vielen Quadratkilometern, wenn du inaktiv in einer LA registriert bist, und einmal einem bis unter 50 Meter genauem Ort, wenn du telefonierst. Die genauen Entfernungen hängen von der Dichte der Antennen ab. Logischerweise ist das in einer Großstadt präziser als auf dem Land.

9.7 Die stille SMS

Weil dein genauer Aufenthaltsort gar nicht bekannt ist, wenn du das Telefon zwar anhast, aber nicht telefonierst (jedenfalls nicht so genau, dass ein Observationsteam dich in einer Großstadt findet,) hat die Polizei ein trickreiches Mittel erfunden:

Die stille SMS
Sie wird gerne eingesetzt, um dich zur orten, wenn dein Mobiltelefon eine Zeit lang inaktiv war und du dich nicht in eine spezielle Funkzelle, sondern nur allgemein in die „Local Area“ eingeloggt bist.

Die Polizei macht sich dabei eine Technik zunutze, die eigentlich von den Mobilfunkfirmen entwickelt wurde, um die Funktionsfähigkeit von Geräten zu testen, ohne dass dabei „offizielle“ Kommunikation entsteht, denn die „stille SMS“ wird von Mobiltelefonen nicht angezeigt. Mit eigens dafür entwickelten Programmen wie „Stealth Ping“ oder „SMS Blast“ schickt die Polizei dabei eine SMS auf dein Mobiltelefon, die so programmiert ist, dass dein Mobiltelefon zwar ein kurzes Antwortsignal sendet, den ganzen Vorgang aber nicht anzeigt.

Dieses Antwortsignal erzeugt die nötigen Daten: Wann Du Dich wo befunden hast. Rechtlich betrachtet gilt das als Telefonverkehr, bei dem die Mobilfunkfirmen verpflichtet sind, sie der Polizei mitzuteilen. Auf diese Weise erhalten diese Schnüffler genaue Angaben über deinen Aufenthaltsort, selbst, wenn du denkst, dass du dein Mobiltelefon gar nicht benutzt hast. Allerdings funktioniert die stille SMS natürlich nur, wenn du das Telefon eingeschaltet hast.

Für die Polizei ist die stille SMS nicht nur eine gute Fahndungsmöglichkeit, sonder auch ein Trick, um die rechtlichen Hürden zu umgehen. Das Abhören von Mobiltelefonen ist nur bei schweren Straftaten möglich, wo für eine richterliche Anordnung gebraucht wird. Die Verbindungsdaten dürfen die Herren in Grün aber seit einiger Zeit bereits bei Straftaten von „erheblicher Bedeutung“ nutzen - also bei einer niedrigeren Schwelle. Die „stille SMS“ ist so mittlerweile zu einem Standardwerkzeug der Bullen geworden.

9.8 Der IMSI - Catcher

Seit einigen Jahren gibt es den sogenannten IMSI-Catcher, ein neuartiges Instrument, das der Polizei hilft, im „Handy-Zeitalter“ durchzublicken und das ein effektives Werkzeug zum Identifizieren von anonymen Mobiltelefonen ist.

Der IMSI-Catcher ist ein kofferraumgroßes Spielzeug, das die Polizei bei Observationen dabei hat, wenn sie wissen wollen, mit welchen Mobiltelefonen du so telefonierst. Telefone, die auf deinen Namen angemeldet sind, sind schnell identifiziert, indem diese Schnüffler in den Kundendienst der Telefonfirmen schauen. Anschließend beantragen sie beim Richter eine Abhörgenehmigung und sind ab da an in der Leitung.

Aber was tun bei anonymen Mobiltelefonen oder von Freund oder Freundin geliehenen Telefonen? In diesen Fällen observieren die Polizeibeamten dich mit einem IMSI-Catcher ein paar Tage lang, um herauszufinden, wie du kommunizierst. Immer, wenn sie dich telefonieren sehen, schalten sie den IMSI-Catcher ein.

Technisch funktioniert das Gerät so, dass es eine Funkzelle der Mobilfunk-Betreiber simuliert. Das heißt, dein Telefon loggt sich nicht beim nächsten Telekom-Funkmast ein, sondern beim IMSI-Catcher - ohne es zu merken! Der IMSI-Catcher zieht sozusagen magnetisch die Signale aller Telefone im Umkreis von einigen 100 Metern an. Weil die Mobiltelefone denken, sie würden mit einem normalen Funkmast kommunizieren, identifizieren sie sich artig mit ihrer IMSI und ihrer IMEI - und schon wissen Schnüffler, mit welchen Geräten du telefonierst.

Zum IMSI-Catcher gehört ein Computerbildschirm, auf dem alle Telefonnummern im Umkreis erscheinen. Das können in der Einkaufspassage schon mal ein paar Dutzend oder Hundert Mobiltelefone sein. Deshalb folgen sie dir eine Weile und machen an verschiedensten Orten den Catcher an. So reduziert sich der Kreis der möglichen Telefonnummern, die an allen Orten eingeloggt sind, immer weiter, bis nur noch deine Nummer über bleibt.

Rechtlich ist es so, dass der IMSI-Catcher schon seit Jahren eingesetzt wird, aber erst seit 2002 erlaubt ist. Allerdings dürfen die Polizisten auf diese Weise nur deine Nummer herausfinden und dich noch nicht abhören. Deshalb gehen sie, wenn sie dein Mobiltelefon identifiziert haben, anschließend zum Richter und beantragen eine Abhörgenehmigung, um möglichst bald in der Leitung zu sein dich abzuhören. Technisch ist es heute allerdings bereits möglich, mit dem IMSI-Catcher nicht nur die Nummer zu erkennen, sondern auch mit zuhören.

Entscheide selbst, wie hoch die Wahrscheinlichkeit ist, dass die Observateure nicht ab und zu mal rein hören, was da so gesprochen wird ... .

9.9 Was heisst das? Ein Beispiel ...

Wie ausgeführt, sind über das Mobiltelefon verschiedenste Dinge möglich, nicht nur das Belauschen von Gesprächen.

Die eigentlichen Telefonate haben heute gar keine so große Bedeutung mehr. Viel wichtiger sind die Abfalldaten:

Wer Telefoniert mit wem?
Welche Bewegungsprofile entstehen?
Wer benutzt welche, nicht auf sich angemeldete Mobiltelefone?
Und welche Namen und Nummern sind im Adressbuch gespeichert?

Du solltest dich vor allem verdeutlichen, dass deine Geräte Datenabdrücke hinterlassen, die im Zeitalter des Computers natürlich noch lange nachverfolgt werden können.

Anhand eines fiktives Szenarios wollen wir mal verdeutlichen, was das Mobiltelefon so alles anrichten kann, wenn du es unachtsam gebrauchst:

- Der Aktivist Arthur (der in diesem Beispiel zwar den Mund am Telefon hält, aber leider unvorsichtig mit seinem Gerät umgeht), ist ins Visier der Ermittler geraten. Er war einigermaßen clever und hat ein Telefon, das auf seine Mutter angemeldet ist. Deshalb läuft eine Anfrage der Polizei bei T-Mobile, 02, E-Plus und Vodafone ins Leere. Weil Arthur aber als Kontaktperson einer untergetauchten Freundin unter Beobachtung steht, folgt ihm ein paar Tage lang ein Oberservationsteam des Staatsschutzes, um rauszufinden, wie interessant Arthur ist. Die Polizisten haben einen IMSI-Catcher dabei, den sie einmal vor der Kneipe, einmal vor der Wohnung und einmal am Hafen anmachen.
- Zwei Nummern erscheinen bei allen drei IMSI-Attacken auf dem Bildschirm: Die von Arthurs Mutter, die ab sofort abgehört wird, und eine Zweite, unbekannte, die als Prepaid-Karte noch nicht registriert ist. Auch sie wird von diesem Zeitpunkt an abgehört.
- Am Telefon selbst ist Arthur sehr vorsichtig und bespricht nichts politisch Relevantes. So kommen die Schnüffler also nicht weiter. Weil sie aber überprüfen wollen, ob Arthur an der Aktion einer nationalen Gruppe teilgenommen hat, wegen der seine Freundin gesucht wird, beantragen sie rückwirkend die Verbindungsdaten des Gerätes:
- Mit wem ist von diesem Mobiltelefon aus gesprochen worden?
- Die Mobilfunkfirma liefert jetzt nicht nur die Verbindungsdaten, sondern auch die Logfiles, mit denen sich mit einiger Mühe ein ziemlich genaues Bewegungsprofil erstellen lässt. Ganz nebenbei (siehe oben) können diese Schnüffler anhand der IMEI auch ablesen, das Arthur sein Telefon aus Holland hat.
- Die Staatsschutzbeamten waren gründlich und haben (über Anfragen bei den Mobilfunkfirmen und den IMSI-Catcher) nicht nur rausgefunden, welche Mobiltelefone Arthur benutzt. Sie haben auch rückwirkend bei der Mobilfunkfirma die Daten einer bestimmten BSS und der zugehörigen Antennen beantragt, die ganz in der Nähe liegt, wo es vor einem Jahr zu einer Straftat kam. Da die Aktion nachts um 4 Uhr stattfand, sind kaum Daten gespeichert. Allerdings war zum Zeitpunkt der Aktion das Prepaid-Telefon von Arthur eingeloggt, das nicht registriert war und zu dem die Schnüffler deshalb keinen Nutzer zuordnen können. Dank des IMSI-Catchers wissen sie jetzt, dass das Mobiltelefon von Arthur benutzt wird.
- Aus den Daten der Mobilfunkfirma wissen die Beamten auch, dass das Gerät in der betreffenden Nacht nur zwei Mal kurz genutzt wurde, ohne dass ein Gespräch zustande kam. Da aber auch Anwahlversuche gespeichert werden, wissen sie immerhin, mit welcher anderen

Nummern Arthur nachts telefonieren wollte. Sie vermuten, dass die zweite Person ebenfalls an der Aktion beteiligt war und das Anklingeln ohne zu reden ein verabredetes Signal war.

- Durch die rückwirkend gelieferten Daten sehen die Polizisten auch, dass das auf Arthurs Mutter registriertes Telefon an einem Samstagabend vor vier Wochen in der Nähe eines Klubs in Berlin eingeloggt war. Dort fand eine nationale Infoveranstaltung zu einigen geplanten Aktionen statt, an der Arthur offenbar teilgenommen hat. Erst am Montag drauf war er wieder zu Hause in Hamburg. Aufgrund der neu gewonnenen Erkenntnisse wird Arthur observiert.
- Arthur bemerkt die unauffälligen Herren in ebenfalls so unauffälligen Opel Astras und schlägt ein paar Haken in der U-Bahn und bei Saturn, bis er sicher ist, alleine zu sein. Die Observateure schicken, nachdem sie Arthur verloren haben, eine stille SMS an die Nummer ... siehe da: Arthur hat das Telefon seiner Mutter eingeschaltet gelassen!
- Auf dem Display sehen die Observateure deshalb, in welcher Funkzelle das Mobiltelefon eingeloggt ist.
- Ein paar Minuten später haben sie Arthur wiedergefunden. Um nicht erneut aufzufallen, bleiben die Observateure ab sofort außer Sichtkontakt, überprüfen aber regelmäßig mittels stiller SMS den Aufenthaltsort des Telefons.
- Bei einem NPD-Infostand, an der Arthur teilnimmt, nehmen die Polizisten ihn schließlich hoch. Weil die Polizei bei der anschließenden Hausdurchsuchung die PIN-Nummer seines Telefons finden, kopieren sie als Erstes das gesamte Telefon-Adressbuch und werten es anschließend aus. Auf diese Weise haben sie nicht nur ein umfassendes Bewegungsprofil von Arthur erhalten, sonder können auch präzise sehen, mit wem Arthur wie oft Kontakt hält. Theoretisch könnten sie das gleiche jetzt mit allen so erlangten Nummern machen - was in der Praxis natürlich nur in ausgewählten Fällen gemacht wird.

Das Beispiel ist konstruiert und klingt sehr übertrieben. Es soll aber vor Augen führen, was theoretisch alles geht (und praktisch oft auch gemacht wird).
Halte dir immer vor Augen, dass neben dem Inhalt von abgehörten Gesprächen auch ein breites Bewegungsprofil von dir entsteht, wenn du Mobiltelefone nutzt - aktuell, aber auch rückwirkend!

9.10 Zusammenfassung

Kurz zusammengefasst bedeutet das Mobiltelefon für dich:

1. **Bei heiklen Aktionen solltest du generell kein Telefon dabei haben.**
2. **Mache das Telefon bei sensiblen Gesprächen aus und entferne den Akku!**
3. **Rücke nie freiwillig die PIN raus!**
4. **Verwende vorhandene Sicherheitsmechanismen (z.B. Kennwortschutz, Verschlüsselung des Adressbuches)**
5. **Mache dein Mobiltelefon nicht nur während eines Treffens aus, sondern deutlich vorher und nachher, so dass dein Aufenthaltsort nicht rekonstruierbar wird!**
6. **Wenn du Mobiltelefone bei heiklen Aktionen einsetzten willst, bleibt nur ein sicherer Weg: Ganz neue Mobiltelefone und SIM-Karten zu nehmen, die weder vorher noch nachher benutzt wurden oder werden.**
7. **Gerät vor Verlust schützen**

9.11 Smartphone Sicherheit

Es gibt kaum noch Menschen, die kein Smartphone nutzen. Laut Larry Page, dem Mitbegründer von Google, wurde Android als Betriebssystem auf rund 750 Millionen Geräten weltweit aktiviert. Damit nutzen rund 75 Prozent aller Smartphone-User weltweit Android, rund 15 Prozent Apples iOS. Kurz gesagt heißt das nichts anderes als: Je verbreiteter ein Betriebssystem ist, egal ob auf dem Computer oder Smartphone, desto attraktiver wird dieser Umstand für Kriminelle, um an Daten oder sogar an Geld zu kommen.

Und das wiederum bedeutet, dass es mittlerweile mehr als sinnvoll ist, sein Smartphone genau wie den stationären Computer gegen digitale Schädlinge aller Art zu schützen.

Sicherheitsexperten mahnen schon seit Jahren Datenschutz auch auf dem Mobiltelefon an und warnen vor Handy-Kriminalität. Nur interessierte das bisher kaum jemanden. Denn ein Smartphone vermittelt eine Art „gefühlte Sicherheit“: Es ist klein, man hats im Blick, was soll da schon passieren ...

Der Mobilfunkanbieter weiß, von wo aus du wen angerufen und an wen du eine SMS gesendet hast. Das Handy protokolliert die Daten mit und kann sie versenden. Wer auch das Weltnetz mobil nutzt, gibt seine IP-Adresse preis, und das gleich in mehreren (WLAN-) Netzen. Munter werden oft dutzende Apps ohne jede Prüfung installiert und Daten sind im Klartext und ohne Schutz gespeichert. Schadprogramme wie Viren oder Trojaner haben da leichtes Spiel. Und schließlich Diebstahl: Ist das Telefon weg, sind alle Daten leichte Beute.

9.12 Sicherheitslücken von Smartphones stopfen

Jeder ist mittlerweile mehr oder weniger ständig online und nutzt neben Computer und Notebook auch leistungsfähige Smartphones für eine immer größer werdende Anzahl von Tätigkeiten. Je wichtiger Mobilgeräte für uns sind, desto interessanter werden sie als Ziele für Internetkriminelle.

Gleichermaßen wichtig sollte jedem die Sicherheit der eigenen Geräte sein, doch laut der MCSI-Studie von Microsoft machen sich 77 Prozent aller Anwender keine Sorgen - ein gefährlicher Leichtsinn, denn Schädlinge wie Viren, Trojaner und Rootkits stellen neben Computer und Notebook auch für Mobilgeräte wie Smartphones eine immer größere Gefahr dar. Was man tun kann, um sich schon im Voraus zu schützen, verraten wir im Folgenden.

Augen auf beim App Download
Bevor du dir eine App herunterlädst, musst du erst feststellen, ob die Quelle vertrauenswürdig ist. Die offizielle Weltnetzseite des Entwicklers ist dabei immer einen ersten Blick wert. Diese ist direkt in allen App Stores verlinkt. Wenn sich dort keine seriöse Weltnetztseite mit Impressum befindet, ist Vorsicht geboten.

Hilfreich ist hierbei das Prädikat „Top-Entwickler“, das etwa Google in seinem Play Store für ausgewählte Software-Hersteller vergibt, die nicht nur hochwertige Qualität abliefern, sondern auch besonders vertrauenswürdig sind. Das Qualitätssiegel findet man unter dem Namen des Entwicklers auf der App-Seite.

Unnötige Risiken vermeiden
Ebenfalls empfehlenswert ist, die Installation außerhalb des jeweils offiziellen App Stores standardmäßig zu unterbinden. Dies betrifft insbesondere Android- Smartphones, da Google alternative Quellen zulässt. Solche Android-Apps im APK-Dateiformat kann man etwa per eBrief, von der Weltnetzseite des Entwicklers oder aus einem alternativen App Store erhalten.

Um zu verhindern, dass etwa ein böswilliges Programm auf diesem Weg in der Lage ist, ungefragt

Apps zu installieren, entferne unter „Einstellungen / Sicherheit“ den Haken bei „Unbekannte Quellen“. Natürlich sind alternative App Stores nicht grundsätzlich eine Gefahr oder schlechter als das Original, wie Amazon und AndroidPIT beweisen. Falls du also doch einmal eine APK-Datei installieren willst, kannst du die obige Option vorübergehend reaktivieren.

Es versteht sich von selbst, dass du Raubkopien von Apps und Software in jedem Fall vermeiden solltest. Solche werden über rechtswidrige Quellen im Weltnetz zugänglich gemacht, sind aber potenzielle Malware-Fallen. Besonders im Bereich mobiler Apps lohnt sich dieses enorme Risiko nun wirklich nicht, besonders wenn man bedenkt, dass es sich meist um eine Ersparnis von nur wenigen Euro handelt. Berechtigungen als Einfallstor zum Mobilgerät

Überprüfe vor dem Download die Berechtigungen, die eine App während der Installation anfordert. Je nach Programm sind Weltnetzzugang und Zugriff auf den internen Speicher normale Berechtigungen, ohne die viele Apps nicht funktionieren. Auch beim Thema Ortsdaten solltest du sensibel sein - diese dienen kostenlosen Apps zur gezielten Schaltung von Werbung.

Wenn eine App aber ohne ersichtlichen Grund das Google-Konto, die Kontakte oder den Telefonstatus anzapfen möchte, sollten die Alarmglocken läuten. Im Zweifelsfall sollte man auf die Installation der App lieber verzichten.

Kein Verzug bei Updates
Selbst wenn du bei der Installation von Software und Apps größte Sorgfalt geleistet hast, besteht die Gefahr von Programmierfehlern und Sicherheitslücken.

Besitzer von Smartphones sollten ihre Apps regelmäßig auf den neuesten Stand bringen. Rufe dazu die jeweilige App-Store-App unter „Meine Apps“ auf. Über die Funktion „Alle aktualisieren“ lassen sich dann alle betroffenen Apps mit einem Fingertipp aktualisieren. Dies sollte man möglichst im WLAN machen, um das mobile Datenvolumen zu schonen.

Sobald du deine Apps im Griff hast, bist du schon einmal vor dem schlimmsten Gefahrenherd für dein Smartphone geschützt. Dennoch verbleiben einige wichtige Vorbereitungen, damit du auch in jeder Situation geschützt bist: Offizielle Updates für dein Betriebssystem stehen hierbei ganz oben auf der Liste. Leider unterstützen nicht alle Firmen automatische Patches, sodass du unter Umständen auf der offiziellen Seite deines Geräteherstellers nachsehen musst.

Schutz vor Langfingern
Am einfachsten schützt du deine Daten vor neugierigen Blicken oder Dieben, indem du den Lockscreen des Smartphones mit einem Passwort schützt. Die Sicherung durch das Zeichnen einer Geste oder gar keine Sicherung ist weitaus beliebter. Durch Verschmierungen auf dem Bildschirm lässt sich die Geste aber nicht selten nachvollziehen.

Für den Fall, dass dein Gerät abhanden kommt, gibt es Anti-Diebstahl-Apps für dein Telefon. Die App von Antivirus-Hersteller Lookout zum Beispiel peilt dein Gerät per Google Maps an, kann einen Alarm aussenden oder ein Bild von der Person machen, die das Gerät benutzt. Sogar eine Fernverschlüsselung oder gar eine Systemzurücksetzung aus der Ferne sind möglich - allerdings nur für die Premium-Version der App.

Sensible Daten verschlüsseln
Speichere so wenig persönliche Informationen wie möglich auf deinem Gerät: Passwörter oder Kreditkarten-Daten haben nichts auf dem Gerätespeicher verloren. Ist man darauf angewiesen, Zugriff auf wichtige Daten zu haben, sollte man diese veschlüsseln.

Wer seine Passwörter lieber lokal speichert, sollte das Tool KeePass verwenden. Diesen gibt es sowohl für Windows als auch für Mobilgeräte. Die damit erzeugte Passwort-Datenbank lässt sich

auch auf mobilen Geräten öffnen: Mit KeePassDroid (Android), MiniKeePass (iPhone) und 7Pass (Windows Phone 7/8) stehen passende mobile Apps bereit.

Sensible Dokumente sollte man auf dem Smartphone nur verschlüsselt speichern. Das funktioniert sehr einfach mit Note Cipher. Geht das Smartphone verloren, sind zumindest die verschlüsselt gespeicherten Daten sicher vor Missbrauch geschützt.

Richtiges Verhalten am WLAN-Hotspot
Im Gegensatz zum privaten WLAN ist ein öffentlicher Hotspot (etwa in der Hotel-Lobby, im Café oder Restaurant) unverschlüsselt und steht jedem Anwender offen. Mit geeigneten Hilfsmitteln kann ein Mitnutzer dieses Hotspots deinen Datenverkehr belauschen und auf diese Weise etwa deine Zugangsdaten für eBriefe, Foren oder das Online-Banking abhören.

Noch dreister: Der Datendieb errichtet - etwa mit seinem Notebook - selbst einen freien Pseudo-Hotspot, der allein dazu dient, die Datenströme aller Opfer abzuhören, die sich in diese Falle einloggen.

Deaktiviere das GPS
Bei einer Demonstration hat die Polizei durch Auswertung der Mobilfunkzellendaten Handybesitzer ausspioniert: eingehende und ausgehende Anrufe, SMS und Position. Begründung: Damit sollen Drahtzieher von schweren Straftaten und Mitglieder einer kriminellen Vereinigung überführt werden. Neben dem Mobilfunkanbieter haben also auch staatliche Stellen (mit richterlicher Genehmigung) Zugriff auf Handydaten. Dagegen ist niemand gefeit.

Einzige Abhilfe: das Smartphone ausgeschaltet zu Hause lassen.
Davor hatte Apple für heftige Negativ-Nachrichten gesorgt: iPhones und iPads zeichnen die per GPS ermittelten Standorte der Besitzer auf und übermitteln diese Daten an Apple-Server im Internet. Die GPS-Datensammlung über das Handy ist aber schon lange üblich. Eingebaute standortbezogene Dienste wie etwa Karten zur Navigation, die Ortung von Familienmitgliedern und Touristeninfos brauchen GPS-Daten, um zu funktionieren. Diese Standortdaten lassen sich leicht auch dazu verwenden, lokalisierte Werbung einzublenden.

Deaktiviert man die Ortungsdienste über das Einstellungsmenü des Smartphones, dürfen Gerät und Apps den Standort zwar nicht mehr übermitteln, jedoch werden Diese Daten dennoch weiter im Hintergrund auf dem Gerät gespeichert. Größter Haken der Abschaltung neben dem Nutzenverlust: Die Geräte laufen nicht mehr fehlerfrei. Wer standortbasierte Dienste als Dreh- und Angelpunkt seiner Handynutzung begreift, kann also Rückschlüsse auf seinen Standort nicht verhindern.

Weniger ist mehr
Gegen die Datensammelei hilft wenig: private Nachrichten öfter auf deinen Computer überspielen, nur das Nötigste auf dem Handy lassen. Und wer gerne mit dem Smartphone ins Weltnetz geht und sich in sozialen Netzwerken tummelt, sollte Privates nach Möglichkeit nur anonymisiert per Pseudonym von sich geben. Die oft ständig aktivierte Bluetooth- und WLAN-Technik ist ebenfalls sicherheitsbedenklich: Hacker könnten vor allem über Bluetooth-Funk ins Mobiltelefon einbrechen und private Daten abgreifen oder kostenpflichtige Nummern anrufen. Daher sollten diese Verbindungsarten nur aktiviert sein, wenn sie nötig sind.

Trojaner und Phishing-Internetadressen werden gern über eBriefe verbreitet. Daher gilt beim Smartphone wie am Computer: Keine eBrief-Anhänge und keine Weltnetzempfehlungen von Unbekannten öffnen. Bei Apps sollte man genau hinsehen, worauf sie zugreifen wollen, und sie nur aus seriösen Quellen installieren. Tests und Nutzerkommentare in den App-Märkten helfen, Datensammler zu entdecken.

Plötzlich erhöhter Datenverkehr oder eine zu hohe Abrechnung können Indizien für Schadpro-

gramme sein. Ein Zurückstellen des Mobiltelefons auf die Werkseinstellungen ist eine radikale Gegenwehr, aber manchmal nötig. Gut ist, wenn man für diesen Fall regelmäßig alle Daten sichert.

Niemals ohne Schutz
„Installiere eine Sicherheitssoftware“ - diese Binsenweisheit sollte eigentlich jedem Computer-Besitzer vertraut sein, doch die Realität sieht anders aus. Nach der bereits zu Beginn erwähnten Microsoft-Studie haben lediglich 56 Prozent der Computer-Anwender eine Antiviren-Software installiert, 44 Prozent surfen infolgedessen ungeschützt durchs Weltnetz.

Dabei lässt sich dieser Leichtsinn leicht unterbinden: Gute Antiviren-Software bekommt man sogar kostenlos, etwa „AntiVir“. Auf Mobilgeräten sieht die Quote noch schlechter aus, doch auch hier gibt es sehr guten Schutz gratis. Mehr dazu im Artikel Antivirus.

Sehr empfehlenswert sind die Verschlüsselung privater Daten und regelmäßige Backups - auf den eigenen Computer. Gegen Verlust oder Diebstahl des Smartphones ist meißt kein Kraut gewachsen. Rückverfolgungsprogramme funktionieren nur, wenn sie aktiv sind und das Handy an ist.

Bei einer unbefugten SIM-Karte wird dann per SMS die Mobiltelefon- und die IMEI-Nummer von der neuen SIM-Karte an eine vorher festgelegte Telefonnummer geschickt. Andernfalls hilft nur, die SIM-Karte über die Servicestelle oder Weltnetzseite des Mobilfunkanbieters zu sperren. Das ist dazu nötig: Rufnummer, Kundennummer und -kennwort sowie die IMEI (eindeutige Mobiltelefon-Seriennummer), die über den Code *#06# abrufbar ist.

9.13 Android Berechtigungen - Alles oder nichts

Android nutzt ein Unix-ähnliches System, um die Berechtigungen von Apps zu verwalten. Vor der Installation einer jeden App werden die benötigten Berechtigungen aufgelistet und mit vagen Worten beschrieben. Im Normalfall versteht der Anwender nicht, warum eine App die geforderten Berechtigungen benötigt. Meistens ist es ihm auch herzlich egal - immerhin hält ihn nur noch ein Fingertipp von der Installation ab. Dabei gilt das Prinzip: „Alles oder nichts“. Entweder die Berechtigungen der App werden akzeptiert oder eine Installation ist nicht möglich.

Android Nutzergruppen
Faszination Apps. Was bewegt jemanden dazu eine App zu installieren? Ist es die Aufmachung, eine Empfehlung eines Freundes oder einfach nur Neugier? Selten war es so einfach etwas zu konsumieren. Binnen eines Augenblicks ist die App auf dem Gerät installiert und kann benutzt werden.
Was bewegt Menschen zu diesem sorglosen Umgang mit der Technik, die sie kaum verstehen? Jeder Android-Nutzer kommt zwar fast täglich mit den Berechtigungen in Berührung, aber nur die wenigsten hinterfragen auch was wirklich dahinter steckt. Um das besser zu verstehen beginne ich den Beitrag mit einer kleinen Parodie über verschiedene Nutzergruppen.

- Android-Neuling
  Ein Android-Neueinsteiger hält zum ersten Mal sein Gerät in der Hand und versucht eine App zu installieren. Vor der Installation hüpft ihm ein Popup entgegen - folgende Berechtigungen sind zu akzeptieren, ansonsten ist eine Installation nicht möglich. Wird schon schiefgehen, immerhin handelt es sich hierbei um eine App aus dem Google Play Store und die sind doch sicherlich geprüft! Also schnell abnicken - die App ist installiert. Den Berechtigungen wurde nicht ein Hauch von Aufmerksamkeit geschenkt.

- Android-Nutzer
  Nach ein paar Wochen kennt man sich schon etwas mit dem System aus. Mittlerweile tummeln sich zahlreiche Apps auf dem Gerät und es werden immer mehr. In Communities, Foren oder News-Seiten werden brandneue Apps vorgestellt, die der Nutzer dann sogleich ausprobieren will / muss. Bunte Bildchen, tolle Funktionen und vor allem kostenlos. Damit wird

der Nutzer gelockt. Ein Blick auf die Berechtigungen werfen vor der Installation? Wozu? Die App wurde doch empfohlen und zudem wird sie im Google Play Store angeboten.

- Android-Fortgeschrittener
  Der App-Konsum nimmt langsam ab. Man muss sich wirklich nicht mehr jeden Mist installieren. Die Benutzung beschränkt sich mittlerweile auf Apps die man mag und die sich gut in den täglichen Tagesablauf integrieren lassen. Von Berechtigungen hat diese Nutzergruppe auch schon etwas gehört. Hier und da liest man in einschlägigen online Medien wieder über den Selbstbedienungsladen Smartphone - bzw. wie Apps ihre Nutzer ausspionieren. Das regt zum nachdenken an und lässt die ein oder andere App wieder vom Gerät verschwinden. Eventuell ist das Gerät gerootet und das ein oder andere Custom-ROM wurde auch schon mal probiert. Wobei die schlechten Erinnerungen überwiegen. Irgendwie waren da alle Daten weg...

- Android-Experte
  Alles schon gelesen und ausprobiert. Das Gerät ist mit Sicherheit gerootet und ein Custom-ROM werkelt auf dem Gerät. Neben dem Austausch mit anderen Entwicklern im xda-Forum kompiliert gerade die neue App. Dieser Nutzer verfügt über ein hohes technisches Verständnis und opfert einen Großteil seiner Freizeit der Android Community. Android-Experten sind sich der Gefahr bewusst, die von Berechtigungen ausgehen können.

- Android-Paranoider
  Vergleichbar mit einem Android-Experten verfügt der Paranoide über ein hohes Maß an technischem Verständnis. Sein Gerät ist ebenfalls gerootet und mit einem Custom-ROM bestückt. Zusätzlich schützt er sich mit diversen Tools vor der Ausbeutung seiner persönlichen Daten. Zur Grundausstattung gehört zweifellos eine Firewall und ein Berechtigungsmanager. Berechtigungen und ihre Bedeutung kennt er auswendig. Vor jeder Installation einer App werden die angeforderten Berechtigungen penibel geprüft.

Android Berechtigungen

- Ein Designfehler
  In ihrer Grundidee sollen Berechtigungen auf Android gewährleisten, dass Apps ohne explizite Rechte keinerlei Aktionen auf dem Gerät ausführen dürfen. Vor der Installation wird daher ein Fenster eingeblendet, welches den Nutzer über die angeforderten Berechtigungen informiert. Die Verantwortung wird hierbei in die Hände des Nutzers gelegt. Gefallen ihm die Berechtigungen nicht, kann er noch immer ablehnen und die App nicht installieren. Auf den ersten Blick ein vernünftiges System, das in der Praxis allerdings kaum funktioniert.

  Der Nutzer hat sich das Gerät zugelegt, weil er sich dadurch eine einfache Handhabung erhofft und nicht um sich anschließend mit Berechtigungen herumzuschlagen, die er sowieso nicht versteht. Es ist paradox. Hersteller sind in der Lage die Systeme so zu konzipieren, dass der Umgang heutzutage tatsächlich kinderleicht ist. Auf der anderen Seite haben sie kein Interesse oder sind schlichtweg nicht dazu in der Lage Privacy by Design zu implementieren.

  Halten wir also nochmal fest: Ja es existiert eine Sicherheitsfrage vor der Installation einer App, allerdings ist der Großteil der Anwender damit schlichtweg überfordert. Also wird die App installiert und man verlässt sich auf sein System. Im Nachhinein hat man keinerlei Möglichkeiten die benötigten Berechtigungen zu kontrollieren bzw. erhält keinen optischen Hinweis, falls tatsächlich ein Zugriff auf sensible Informationen stattfindet. Hier vereinen sich zwei Welten miteinander. Die Unbedarftheit der Anwender und die (gewollte) Unfähigkeit der Hersteller.

- Datenschleudern
  An dieser Stelle möchte ich nicht jede einzelne Berechtigung im Detail beleuchten oder was damit theoretisch möglich wäre. Nico Heister von AndroidPIT hat das in einem Beitrag

schon sehr gut zusammengefasst. Wer darüber hinaus noch Informationen benötigt, der sollte einfach direkt bei den Entwicklern nachfragen, warum eine App gerade diese Berechtigung benötigt. Einige Entwickler haben das Problem mit den Berechtigungen erkannt und versorgen den Benutzer mit detaillierten Informationen. Beispiele

Immer wieder finden dubiose Apps ihren Weg in den Android Markt. Daneben existieren ebenfalls seriöse Apps die Zugriff auf sensible Informationen verlangen. Im Folgenden beschränken wir uns auf eine kurze Auflistung von Beispielen. Hierbei handelt es sich um einen Ausschnitt, die Dunkelziffer liegt mit Sicherheit höher.

Selbstbedienungsladen Smartphone (heise)
Neue Android-App will mithören (heise)
Smartphone-App Path lädt heimlich Adressbuch hoch (PCWelt)
Smartphone-User klagen über Adressbuch-Greifer (Spiegel Online)
Wie Facebook private Telefonbücher abgreift (Spiegel Online)

Taschenlampen App

Was steckt hinter einer Berechtigung? Was könnte eine App damit anstellen? Diese Fragen lassen sich nicht pauschal beantworten. Dazu muss man eine App sehr genau analysieren und gegebenenfalls ihre Kommunikation mit dem Weltnetz mitschneiden. Anhand von der App Taschenlampe - Tiny Flashlight möchten wir dies veranschaulichen.

Berechtigungen

Die App fordert bei der Installation folgende Berechtigungen an:

Bilder und Videos aufnehmen

Ermöglicht der App, Bilder und Videos mit der Kamera aufzunehmen. Die Berechtigung erlaubt der App, die Kamera jederzeit und ohne deine Bestätigung zu nutzen.

Gutartig: Ohne diese Berechtigung kann die App die interne LED nicht aktivieren. Wird also benötigt, ansonsten leuchtet nichts. Bösartig: Bilder und Videos aus allen Lebenslagen. Noch dazu benötigt die App keine Bestätigung durch den Nutzer.

Voller Netzwerkzugriff

Ermöglicht der App die Erstellung von Netzwerk-Sockets und die Verwendung benutzerdefinierter Netzwerkprotokolle. Der Netzbetrachter und andere Apps bieten die Möglichkeit, Daten über das Weltnetz zu versenden. Daher ist diese Berechtigung nicht erforderlich, um Daten über das Weltnetz versenden zu können.

Gutartig: Die App ist kostenlos und finanziert sich durch die Darstellung von Werbung. Dazu wird Internetzugriff benötigt. Bösartig: Im Hintergrund sammelt die App fleißig persönliche Daten. Dazu gehört bei dieser App die eindeutige IMEI oder IMSI. Zudem kann die App Bilder und Videos aufnehmen - die könnten über diesen Kanal verschickt werden.

Telefonstatus und Identität abrufen

Ermöglicht der App, auf die Telefonfunktionen des Geräts zuzugreifen. Die Berechtigung erlaubt der App, die Telefonnummer und Geräte-IDs zu erfassen, festzustellen, ob gerade ein Gespräch geführt wird, und die Rufnummer verbundener Anrufer zu lesen.

Gutartig: Bei einem Anruf beendet sich die App selbst bzw. unterbricht ihre Arbeit und merkt sich den aktuellen Zustand. Nach dem Telefonat öffnet sich die Taschenlampen App wieder und leuchtet dir den Weg nach Hause... Bösartig: Ermöglicht der App die Erfassung eurer Telefonnummer, der IMEI oder IMSI.

Ruhezustand deaktivieren

Ermöglicht der App, den Ruhezustand des Telefons zu deaktivieren.

Gutartig: Hindert das Smartphone am Standby-Modus. Die Taschenlampe soll natürlich so lange leuchten, bis die App beendet wird oder eine manuelle Sperrung vorgenommen wird.

Bösartig:

Datenanalyse

Man kann dieser App (bzw. Apps) generell jetzt keine böse Absicht unterstellen. Immerhin benötigt eine App bestimmte Berechtigungen, um letztendlich zu funktionieren. Interessant wird es erst dann, wenn der App-Verkehr mitgeschnitten wird. Folgende Verbindungen baut die Taschenlampen-App auf:

*.doubleklick.net
*.flurry.com
*.mydas.mobi

Was verbirgt sich dahinter?

*.doubleklick.net - Wurde von Google gekauft und wird oft mit Spyware in Verbindung gebracht. Ermöglicht eine Aufzeichnung der angezeigten Werbung und welche angeklickt wurde.
*.flurry.com - Sammelt und wertet Daten aus. Deine Daten. Weitere Infos zum Dienst.
*.mydas.mobi - Gehört zu Millennial Media. Ähnlich wie Doubleklick.

Im Google Play Store unter Beschreibung kann ich außer Marketing-Texten keinen Hinweis darauf finden, dass sich die App durch Einblendung von Werbung finanziert. Letztendlich lassen die Berechtigungen zwar darauf schließen, aber sicher sein kann man sich nicht. Schlussfolgerung

In Anbetracht des Datenmitschnitts lautet die Schlussfolgerung: Die App finanziert sich durch Werbung. Dazu sammelt sie persönliche Informationen und schickt diese an doubleklick.net, flurry.com und mydas.mobi. Dort werden diese ausgewertet und mit anderen Daten verknüpft, die beispielsweise von anderen Apps gesammelt wurden. Über die IMEI lässt sich daraus dann schnell ein eindeutiges Profil erzeugen.

Das es auch anders geht beweist die App Search Light. Sie benötigt eine einzige Berechtigung, um zu funktioneren. Wer sich einen Spaß erlauben möchte, der kann sich mal die 100 verschiedenen Taschenlampen-Apps anschauen und deren Berechtigungen vergleichen.

Angeforderte Berechtigungen bei der Installation sind also nicht per se schlecht, allerdings wird der Anwender im Dunkeln gelassen, was eine App damit wirklich anstellt. Dazu sind dann aufwendige Datenmitschnitte notwendig.

Was kannst du tun?
Wem Datenschutz wichtig ist, der steht vor einem Dilemma. Einerseits sind diese Smartphones schick, wunderbar einfach zu bedienen und unübertroffen in ihrer Funktionsvielfalt. Andererseits ist es nahezu unmöglich zu kontrollieren, welche Daten ungefragt das Gerät verlassen. Also lieber

kein Smartphone kaufen? Lieber das alte Nokia 3310 entstauben und dort wieder die SIM-Karte reinstecken? Wer sich an ein paar grundlegende Tipps hält, der kann das Risiko minimieren.

Grundlegende Tipps

Wer sich in Eigenregie vor der Datensammelwut schützen möchte, der sollte folgende Punkte beachten:

- Apps erst gar nicht installieren, die zu viele Berechtigungen einfordern. Dazu ist es allerdings notwendig zu verstehen, welche Aktion eine App durch den Zugriff auf Berechtigung XY durchführen könnte - das macht es kompliziert und nicht wirklich immer transparent. Deshalb helfen Tools, wie aSpotCat die Berechtigungen von Apps genauer zu analysieren.
- Ein weiteres Tool, um im Berechtigungs-Djungel die Übersicht zu behalten, stellt die App APEFS dar. Damit kann gezielt nach Apps gesucht werden, die auf dubiose Berechtigungen verzichten - und das bereits vor der Installation.
- Dennoch bleiben oft Zweifel, die auch nicht immer ausgeräumt werden können. Viele Entwickler haben die Problematik erkannt und legen daher offen, weshalb ihre App Berechtigung XY benötigt.
- Es kann auch sinnvoll sein auf das Bewertungssystem zu achten. Allerdings achtet die Masse nicht wirklich auf die benötigten Berechtigungen. Daher ist dieser Tipp leider nur mit Einschränkung zu genießen.

Selbst wenn diese grundlegenden Hinweise immer eingehalten werden, schützt das nicht automatisch vor schwarzen Schafen. Dazu sind weitere Maßnahmen notwendig. Eine Kombination aus einer Firewall und einem Berechtigungsmanager ermöglichen eine sehr hohe Kontrolle über die eigenen Daten.

9.14 Wichtige APPs für dein Smartphone

Apps sind in aller Munde. Jeder spricht von ihnen. Aber was verbirgt sich eigentlich hinter dem Wort mit den drei Buchstaben? App ist die Kurzform des englischen Wortes „application“ und bedeutet Anwendung. Im allgemeinen Sprachgebrauch sind hiermit Programme, wie Spiele oder Textprogramme, gemeint, die man z.B. auf einem modernen Smartphone oder einem iPad installieren kann.

Die von uns beschriebenen Apps helfen dir deine Wanze, ähm ich meine natürtlich dein Smartphone, etwas sicherer zu gestalten.

9.15 Antivirus

Android ist voll von Malware, Viren und weiteren Gefahren - eine Antivirus-App ist also absolute Pflicht. Untermauert wird diese Aussage / Meinung mit einer Vielzahl bunter Statistiken, die regelmäßig in diversen Studien und Meldungen plakativ Verwendung finden. Falsch sind diese nicht, allerdings furchtbar irreführend und nicht unbedingt realitätsbezogen.

Und doch verbreiten sich solche Statistiken meist wie ein Lauffeuer. Prominente Beispiele hierfür sind die F-Secure Mobile Threat Reports und McAfee Threats Reports. Herausgeber solcher Studien sind meist Antiviren-Software-Hersteller selbst - kann eine unabhängige Berichterstattung wirklich so aussehen? Gerne werden die Studien dann in Artikeln genannt - so auch jüngst beim Spiegel Android ist am meisten von Mobil-Malware bedroht.

So wird also konsequent die Meldung verbreitet, Android sei nicht sicher und habe mit einer anwachsenden Armee von Schadsoftware zu kämpfen. Sind diese Aussagen korrekt oder entsteht hier langsam ein Mythos?

Schadsoftware

Malware sind Programme / Apps, die unerwünschte Funktionen ausführen - Funktionen die der Nutzer eigentlich nicht möchte. Unter dem Überbegriff Schadsoftware werden unterschiedliche Typen zusammengefasst. Dazu gehören beispielsweise:

Computerviren sind die älteste Art von Schadsoftware, sie verbreiten sich, indem sie Kopien von sich selbst in Programme, Dokumente oder Datenträger schreiben. Ein teilweise defektes Virus nennt man „Intended Virus“. Dieses bewirkt meist nur eine »Erstinfektion« einer Datei, ist jedoch nicht fähig sich weiter zu reproduzieren.

Ein Trojanisches Pferd (kurz Trojaner) ist eine Kombination eines (manchmal nur scheinbar) nützlichen Wirtsprogrammes mit einem versteckt arbeitenden, bösartigen Teil, oft Spyware oder eine Backdoor. Ein Trojanisches Pferd verbreitet sich nicht selbst, sondern wirbt mit der Nützlichkeit des Wirtsprogrammes für seine Installation durch den Benutzer.

Spyware und Adware forschen den Computer und das Nutzerverhalten aus und senden die Daten an den Hersteller oder andere Quellen, um diese entweder zu verkaufen oder um gezielt Werbung zu platzieren. Diese Form von Malware wird häufig zusammen mit anderer, nützlicher Software installiert, ohne den Anwender zu fragen und bleibt auch häufig nach deren Deinstallation weiter tätig.

Sandbox

Androids Plattform-Sicherheit basiert auf diversen Komponenten. Einer der Schlüsselfunktionen nennt sich Sandboxing. Jeder Android-App wird vom System eine eindeutige ID (UID) zugewiesen und als separater Prozess ausgeführt. Während der Laufzeit befindet sich eine App also in der Sandbox bzw. Sandkasten - ein isolierter Bereich, innerhalb dessen jegliche Aktion keine Auswirkung auf die Umgebung hat. Standardmäßig kann eine App also nicht mit anderen Apps kommunizieren und hat lediglich begrenzten Zugriff auf bestimmte Bereiche des Betriebssystems.

Möchte App A beispielsweise auf Daten von App B zugreifen oder einen Anruf ohne Berechtigung tätigen, so verhindert das System diesen Zugriff. Alles außerhalb der Sandbox ist für Apps ein Bereich auf den sie keinen Zugriff haben. Wie jedes andere Sicherheitsfeature ist auch das Sandbox-Modell nicht unüberwindbar. Allerdings ist es sehr schwierig für Apps aus dieser auszubrechen, da sie dazu den Linux Kernel von Android kompromittierten müssten.

Es bleibt also festzuhalten: Apps können im Prinzip nicht aus der Sandbox ausbrechen und sind daher prinzipiell nicht in der Lage in das System einzubrechen. Wie also kann Schadsoftware auf ein Android Gerät gelangen und dem System Schaden zufügen?

Panikmache!?
Das soeben vorgestellte Sandbox-Modell von Android verhindert gleichzeitig die Funktion von Antivirus-Apps gegen Schadsoftware. Warum? Sie sind ebenfalls Apps die in einer Sandbox ausgeführt werden und somit keinen Zugriff auf Systemdateien haben. Sie können das System also nicht schützen, weil sie darauf auch überhaupt keinen Zugriff haben. Wie funktionieren Antivirus-Apps also bzw. welche Funktion bieten sie dann überhaupt?

Antivirus-Apps auf Android lesen alle installierten Apps auf einem Gerät aus und prüfen sie im Anschluss gegen eine Liste mit korrupten Apps. Sie beinhalten also eine Datenbank in der Apps

verzeichnet sind, die „bösartige“ Dinge auf dem Smartphone anstellen können. Antivirus-Apps suchen also nicht nach Schädlingen im klassischen Sinne, sondern nach verdächtigen Apps - und diese hat sich der Nutzer selbst installiert!

Im Grunde genommen schützt das Sandboxing-Modell also das Gerät - kann den Nutzer allerdings nicht vor sich selbst schützen. Eine Antivirus-App für Android hat also eine sehr begrenzte Funktionalität. Sie vermitteln sogar eine trügerische Sicherheit - obwohl sie nicht in der Lage sind alle „korrupten“ Apps zuverlässig zu erkennen. Was also tun aus Sicht eines Anwenders? Schadsoftware Beispiele

Findet also eine gezielte Panikmache statt? Und woher kommen eigentlich die Statistiken bzw. auf welcher Grundlage werden diese berechnet? Ein Beispiel:

Sophos meldet die Entdeckung des Trojaners „Andr/Stiniter-A“ im Spiel „The Roar of the Pharaoh“. Die App sei nach der Installation in der Lage sensible Informationen (IMEI, IMSI, Telefon-Nummer, etc.) auszulesen und diese an den Entwickler der App zu schicken. Fakt ist: Die App war niemals offiziell im Google PlayStore zu finden, sondern wurde von diversen Seiten als Download angeboten. Um sich diese Schadsoftware also einzufangen, musste man zunächst eine Webseite aufrufen, die App dort herunterladen und bei der Installation den angeforderten Berechtigungen zustimmen.

Die errechneten Statistiken und Schaubilder in den F-Secure Mobile Threat Reports basieren also auf Apps, die hauptsächlich von dubiosen App Stores und Webseiten bezogen wurden. Diese Schadsoftware existiert also tatsächlich und liefert den Studien die „gewünschten“ Zahlen. Ein kritischer Blick verrät allerdings, dass diese Zahlen kaum in die Realität übertragen werden können. Zudem werden auch Hack-Tools wie DroidSheep zu Malware gezählt - was die Statistik weiterhin verfälscht.

Eines wird zusätzlich gerne verschwiegen: Nutzt ein Anwender ausschließlich das Angebot des Google PlayStores ist die Chance das Gerät mit Malware zu infizieren äußert gering.

Was tut Google?
Google ist sich der gegenwärtigen Situation bzw. Bedrohungslage durchaus bewusst. Android ist aufgrund seines hohen Verbreitungsgrades nunmal Angriffsziel Nummer 1 bei mobilen Betriebssystemen. Entsprechende Gegenmaßnahmen sollen für Sicherheit sorgen:

Bevor eine App in den Google PlayStore gelangt wird sie durch Bouncer automatisch nach Schadsoftware geprüft. Ein Dienst, der jegliche Apps vor der Veröffentlichung prüft und in einer simulierten Umgebung auf das Verhalten untersucht. Sozusagen der erste Schutzwall gegen Schadsoftware im PlayStore. Dennoch gelingt es nicht immer Schadsoftware eindeutig als solche zu identifizieren.

Google ist in der Lage Apps remote zu löschen. Wird eine App also irgendwann als Schadsoftware erkannt, hat Google die Möglichkeit diese vom Gerät zu entfernen.

Seit Android 4.2 werden nicht nur Apps aus dem PlayStore auf Schadsoftware geprüft, sondern auch Apps die von einer beliebigen Quelle bezogen werden - also Sideloading („Installation von anderen Apps aus anderen Quellen als dem Play Store zulassen“).

Ebenfalls seit Android 4.2 werden sogenannte Premium SMS-Nachrichten blockiert. Ursprünglich dient Premium SMS der Abrechnung von Dienstleistungen im Internet oder den Medien. Allerdings wird der Dienst auch genutzt, um versteckt Kosten zu verursachen und Malware-Entwickler zu bereichern.

Das bereits beschriebene Sandbox-Modell schützt das System vor böswilligen Apps. Ein ähnliches

Prinzip hat Google mit den Berechtigungen eingeführt. In ihrer Grundidee sollen Berechtigungen auf Android gewährleisten, dass Apps ohne explizite Berechtigungen keinerlei Aktionen auf dem Gerät ausführen dürfen. Also beispielsweise SMS auslesen oder die aktuelle GPS-Position bestimmen. Gerade aber diese Schutzmaßnahme halte ich für bedenklich. Warum? Das haben wir schon ausführlich im Beitrag Android Berechtigungen - Alles oder nichts erklärt.

Google versucht den Anwender also zu schützen, aber wie immer gilt hier auch eines: Es schützt den Anwender nicht vor sich selbst! Wie kann ich Malware vermeiden?

Android ist von seiner Konzeption ein sehr sicheres Betriebssystem - erfordert dafür allerdings auch das Mitdenken seiner Anwender. Wer sich an folgende Grundregeln hält, reduziert die Wahrscheinlichkeit sich Malware einzufangen fast gegen null:

Die Bezugsquelle für Apps sollte ausschließlich der Google PlayStore darstellen. Im Grunde genommen kann jeder einen Store eröffnen und dort seine Apps anbieten / vermarkten. Dabei ist in vielen Fällen ungeklärt wer hinter dem Angebot steckt oder welche Prüfmethoden verwendet werden, bevor eine App im Store erscheint.

Downloads von Webseiten sind tabu. Es gilt nach wie vor: Als Bezugsquelle für Apps ausschließlich den PlayStore verwenden.

Vor jeder Installation sollten die Berechtigungen geprüft werden - denn auch Google kann einen Store ohne Malware nicht gewährleisten.

Apps die zu viele Berechtigungen bei der Installation einfordern, sollten kritisch hinterfragt werden. Muss eine Taschenlampen-App wirklich meinen aktuelle GPS-Standort wissen und benötigt Netzwerkzugriff? Dazu ist es notwendig die Berechtigungen zu verstehen.

Dennoch bleiben oft Zweifel, die auch nicht immer ausgeräumt werden können. Viele Entwickler haben die Problematik erkannt und legen daher offen, weshalb ihre App Berechtigung XY benötigt.

Deaktivieren der Funktion „Installation von anderen Apps aus anderen Quellen als dem Play Store zulassen“.

Nochmal: Malware für Android existiert tatsächlich - nur nicht in der Relevanz und Häufigkeit wie es uns die Antiviren-Hersteller gerne glauben machen möchten. Wer nicht alle möglichen Apps aus dubiosen Quellen installiert und zumindest kurz über die angeforderten Berechtigungen nachdenkt, der ist im Prinzip auf der sicheren Seite. Mit einer gesunden Portion Menschenverstand und dem Sandbox-Modell hat Malware auf Android nahezu keine Chance - und das sogar vollkommen kostenlos.

Fazit
Sind Antivirus-Apps nun sinnvoll oder nutzlos? Fakt ist: Malware für Android existiert, allerdings nicht in der Relevanz und Ausmaß wie oftmals vermittelt. Hinter Android steckt nunmal ein wachsender Markt, bei dem jeder ein Stück vom Kuchen abbekommen möchte - auch Antiviren-Hersteller. Dem Anwender wird also suggeriert, dass er ohne Antivirus-Apps den bösen Mächten des Internets hilflos ausgeliefert sei.

Neben dem Malware-Schutz werben Antivirus-Apps mit weiteren Funktionen - das war allerdings nicht Fokus des Beitrags. Wer weiterhin mit dem Gedanken spielt sich eine Antivirus-App auf seinem Smartphone zu installieren, dem sei der AV-Test vom März 2013 empfohlen.

Antivirus-Apps bieten bestenfalls einen zusätzlichen Schutz auf den man sich als Anwender allerdings nicht blind verlassen sollte. Viel wichtiger ist der gesunde Menschenverstand und die

Einhaltung einfacher Regeln:

Bezugsquelle für Apps ausschließlich der Google PlayStore.

Vor einer Installation die Berechtigungen prüfen. Sind diese einmal erteilt, dann kann die App auch genau das durchführen. Beispielsweise den GPS-Standort auslesen.

9.16 APG

Bei der Installation von APG gibt es nichts besonderes zu beachten. Die App findest du im Google Play Store. Genauso wie bei K-9 Mail handelt es sich auch hierbei um Open Source Software. Die Weiterentwicklung von APG, „OpenPGP Keychain", wird von K9 leider noch nicht unterstützt, aber APG leistet für uns noch gute Dienste.

Schlüsselpaar generieren
Wer schon ein PGP Schlüsselpaar besitzt, kann diesen Abschnitt überspringen und direkt mit dem Import fortfahren.

Wähle im APG Menü (Menütaste!) den Menüpunkt „Private Schlüssel verwalten" und im darauf folgenden Fenster im Menü „Schlüssel erzeugen".

Mit einem Tipp auf den „Passwort wählen" Button erscheinen zwei Eingabefelder, die du mit einem sicheren Passwort zum Schutz des Private-Keys füllen solltest. Dieses Passwort wird später benötigt, um den Private-Key zum Entschlüsseln von Nachrichten wieder zu entsperren, vergesse es also nicht.

Mit dem „Plus-Button" neben dem Punkt "Benutzer-IDsffügst du eine neue eBriefadresse hinzu, für die die Verschlüsselung funktionieren soll. Jede weitere eBrief Adresse kann mit einem zusätzlichen Druck auf den Plus-Button hinzugefügt werden.

Mit dem Plus-Button neben „Schlüssel" wird ein neuer Schlüssel hinzugefügt. Den Algorithmus knnst du auf „RSA" lassen, aber die Schlüssellänge sollte mehr als 1024 betragen. 2048 Bit oder 4096 Bit sind sicher.

Nach dem Erzeugen des Schlüssels wird festgelegt, wie er verwendet werden soll. Wähle bei der Einstellung „Usage" „Signieren und Verschlüsseln" und als Ablaufdatum des Schlüssels („Expiry") ein Datum, das 3-5 Jahre in der Zukunft liegt. Bis dahin kannst du dir mit dem Schlüsselpaar Nachrichten und Dateien verschlüsseln. Nach Ablauf der Zeit muss ein neues Schlüsselpaar generiert werden.

Noch ein Tipp auf „Speichern" und der Private Schlüssel wird in der Übersicht („Private Schlüssel verwalten") abgelegt. Den dazugehörigen öffentlichen Schlüssel findet ihr im APG Hauptmenü unter „Öffentliche Schlüssel verwalten".

Schlüsselpaar importieren

Wer schon ein PGP Schlüsselpaar besitzt, kann dieses in APG importieren. Dazu werden Public- und Private-Key z.B. via USB auf dem Smartphone abgelegt. In der Übersicht zu den öffentlichen bzw privaten Schlüsseln kann die entsprechende Schlüsseldatei im Menü über den Punkt „Schlüssel importieren" importiert werden.

Schlüssel exportieren

Nachdem ein neues Schlüsselpaar erzeugt wurde, sollten Sicherungen von Public-Key und Private-Key angelegt werden. Abgesehen davon muss der Public-Key sowieso exportiert werden, damit er verbreitet werden kann...

Auf die Exportfunktion bekommst du Zugriff, wenn du einen langen Druck auf den entsprechenden Schlüssel in der Public- und der Private-Key Übersicht machst. („Einzelnen Schlüssel exportieren“). Der Schlüssel im angegebenen Ordner auf dem Smartphone abgelegt.

Nachricht oder Datei verschlüsseln

Die Verschlüsselungsfunktion ist jetzt einsatzbereit und kann nicht nur zum Verschlüsseln von eBriefen und anderen Texten eingesetzt werden, sondern auch zum Verschlüsseln von Dateien wie Fotos, Musik etc. Die entsprechenden Buttons sind im APG Hauptfenster zu sehen. Ich denke, die Einstellungen, die zum Verschlüsseln vorgenommen werden müssen, erklären sich von selbst.

eBriefe verschlüsseln - Integration in K9 Mail

Wie zu Beginn schon erwähnt, kann man APG in den K9 Mailclient integrieren und eBriefe direkt im Client verschlüsseln, ohne dass der Umweg über die „Nachricht verschlüsseln“-Funktion in APG genommen werden muss. Die APG Unterstützung muss in K9 allerdings erst aktiviert werden.

Wechsel in K9 und öffne die Konteneinstellungen eines Kontos deiner Wahl. Im Menüpunkt „Kryptographie“ setzt du den „OpenPGP-Provider“ dann auf „APv“. Damit ist die Verschlüsselung nun möglich. Im Nachrichteneditor werden zwei neue Optionsboxen angezeigt, mit denen du das Unterzeichnen oder Verschlüsseln der aktuellen Nachricht aktivieren kannst. Wurde die Verschlüsselungsoption gesetzt, öffnet sich ein APG Fenster, in dem du den Public-Key des Empfängers auswählst. Dafür muss der Public-Key aber in APG Importiert worden sein. Das kann wie oben erklärt über die Importieren-Funktion von APG passieren, oder über eine Suche auf den Keyservern, auf denen PGP Nutzer ihre Public-Keys ablegen können.

Suche auf Public-Key Servern
APG kann zwar keine Keys auf Server hochladen aber die Suche und der Download von Keys funktioniert. Im Menü des APG Hauptfensters kannst du eine Suche auf einem Keyserver starten. (Button „Key-Server“). Wenn du auf ein Suchergebnis tippst, wird der Public-Key heruntergeladen und in APG importiert, sodass du eine(n) verschlüsselte(n) eBrief, Nachricht oder Datei für diese Person generieren kannst.

9.17 App Guard

Entwickelt wird die Software von der Backes SRT GmbH. Derzeit steht die App in Version 2.4.2 als Direktdownload auf der Herstellerseite zur Verfügung. Für kurze Zeit war die App ebenfalls im Google Play Store erhältlich - wurde dort allerdings von Google wieder entfernt. Vermutlich liegt dies an der Tatsache, dass AppGuard den Quellcode von anderen Apps nachträglich modifiziert und damit gegen Bestimmungen in den Google AGBs verstößt.

Funktionsweise
Die Funktionsweise von AppGuard beschreibt die Backes SRT GmbH wie folgt:

Der SRT AppGuard ist eine Sicherheitssoftware für das mobile Betriebssystem Android. Sie ermöglicht dem Benutzer, das Verhalten von Android Apps von Drittanbietern zu überwachen und gegebenenfalls den Zugriff auf sicherheitskritische Systemressourcen zu verweigern. Der SRT AppGuard implementiert dazu folgende Funktionalität: Der Benutzer wählt eine bereits installierte App aus, die überwacht werden soll. Der SRT AppGuard untersucht den Bytecode (den kompilierten Quellcode) der App und identifiziert jene Instruktionen, die sicherheitsrelevante Funktionen

der Android API (Android-Programmierschnittstelle, -Programmanbindung) aufrufen.

An diesen Stellen fügt der SRT AppGuard zusätzlichen Programmcode ein (Instrumentierung), der den Zugriff auf diese sicherheitsrelevanten Funktionen protokolliert und kontrolliert. Nach Abschluss dieses Prozesses wird die bestehende Original-App deinstalliert und durch die instrumentierte Version ersetzt; dieser Schritt muss durch den Benutzer explizit bestätigt werden.

Nur durch dieses Vorgehen ist die Funktionalität des SRT AppGuard gewährleistet. Sollten Sie mit dieser Funktionalität nicht einverstanden sein, installieren Sie den SRT AppGuard nicht.

Kurz zusammengefasst:

AppGuard untersucht den Bytecode von Apps
Identifiziert dabei sicherheitsrelevante Funktionen
Anschließend fügt AppGuard eigenen Programmcode ein, der sicherheitsrelevante Funktionen protokolliert und kontrolliert.
Die Original-App wird also modifiziert und durch Programmcode ergänzt.
Fazit: Die App verändert den Source Code der Apps und benötigt deshalb auch keinerlei Root-Rechte

Dadurch lässt sich wohl der „Rausschmiss“ aus dem Google Play Store erklären. Bevor wir uns mit den Konsequenzen der Quellcode-Veränderung befassen werfen wir zunächst einen Blick auf die App.
GUI von AppGuard

Nach dem Start befindest du dich auf dem Haupt-Screen. Die App ist übersichtlich und logisch gestaltet - selbsterklärend.

Tippst du auf „Übersicht“ ¿ „Überwacht“ listet dir AppGuard alle überwachten (bzw. modifizierten) Apps auf.

Hinzufügen einer App

Zur Veranschaulichung füge ich, durch einfaches Anklicken der App, „Taschenlampe“ zu den von AppGuard überwachten Apps hinzu.

AppGuard führt drei Schritte durch:

Als erstes wird Taschenlampe nach sicherheitsrelevanten Funktionen gescannt und anschließend ein modifiziertes APK-File erstellt.
Danach erfolgt die Deinstallation von Taschenlampe.
Anschließend wird die durch AppGuard modifizierte Version installiert.

Dabei gehen alle Anwendungsdaten und Einstellungen verloren.

Anschließend kann Taschenlampe durch AppGuard kontrolliert / überwacht werden.

Berechtigungen einschränken
Nach der Modifikation kannst du die Zugriffsrechte einschränken.

Die App hat derzeit Zugriff auf folgende Berechtigungen:

Uneingeschränkter Internetzugriff: Selbsterklärend
Telefonstatus lesen und identifizieren: Wird im Normalfall genutzt, wenn ein Anruf reinkommt.

Die App friert dann ihren aktuellen Zustand ein. Nach dem Telefonat wird der aktuelle Zustand der A
pp wiederhergestellt. Kann auch zum auslesen der IMEI und IMSI genutzt werden. Bilder und Videos aufnehmen: Selbsterklärend
Standby-Modus deaktivieren: Ermöglicht der App das Ausschalten eures Bildschirms zu verhindern.

Das sind die „Maximalrechte“ der App. Sie könnte also auf die eben genannten Informationen zugreifen - oder auch nicht. Analysieren wir mal kurz die Zugriffsrechte aus Sicht des Good- und Bad Cops.

Good Cop vs. Bad Cop
Im folgenden habe ich die Berechtigungen der Taschenlampen App aus der Sicht des Good- und Bad Cops dargestellt. Das sind lediglich Beispiele, spiegeln allerdings oft die Realität wieder.

Uneingeschränkter Internetzugriff:

Good Cop: Die App ist kostenlos und finanziert sich durch die Darstellung von Werbung. Dazu wird Internetzugriff benötigt. Bad Cop: Im Hintergrund sammelt die App fleißig persönliche Daten. Dazu gehört bei dieser App die IMEI oder IMSI und Bilder bzw. Videos die ihr aufgenommen habt. Zusätzlich werden die gesammelten Daten von den Werbeanbietern korreliert. Es entsteht ein Benutzerprofil.

Telefonstatus lesen und identifizieren:

Good Cop: Bei einem Anruf beendet sich die App selbst bzw. unterbricht ihre Arbeit und merkt sich den aktuellen Zustand. Nach dem Telefonat öffnet sich die Taschenlampen App wieder und leuchtet dir den Weg nach Hause... Bad Cop: Liest ganz frech die IMEI und IMSI aus.

Bilder und Videos aufnehmen:

Good Cop: Ohne diese Berechtigung kann die App die interne LED nicht aktvieren. Wird also benötigt, ansonsten leuchtet da gar nichts. Bad Cop: Bilder und Videos aus allen Lebenslagen! Und die werden dann auch brav an den Entwickler geschickt. Der braucht auch mal was zu lachen...

Standby-Modus deaktivieren:

Good Cop: Hindert das Smartphone am Standby-Modus. Die Taschenlampe soll natürlich so lange leuchten, bis die App beendet wird. Bad Cop: Ne - hier ist nichts.

Ist die Taschenlampen App jetzt ein „Good Cop“ oder „Bad Cop“? In diesem Artikel erlaube ich mir kein abschließendes Urteil. Log Datei

Kommen wir noch zu einer sehr sinnvollen Funktion. Im Log können wir sehen, wann die App welche Berechtigung genutzt hat und wohin Internetverbindungen aufbaut wurden.

Im Screenshot sind drei unterschiedliche Verbindungen zu erkennen:

*.doubleklick.net
*.flurry.com
*.mydas.mobi

Eine kurze Analyse:

*.doubleklick.net - Wurde von Google gekauft und wird oft mit Spyware in Verbindung gebracht. Ermöglicht eine Aufzeichnung der angezeigten Werbung und welche angeklickt wurde.
*.flurry.com - Sammelt und wertet Daten aus. Eure Daten. Weitere Infos zum Dienst.
*.mydas.mobi - Gehört zu Millennial Media. Ähnlich zu Doubleklick.

Zwei Dienste zum Einblenden von Werbung und ein Datensammler. Gut zu wissen... Kommen wir nun zu den positiven / negativen
Eigenschaften von AppGuard.
Positiv / Negativ - AppGuard

Zunächst die positiven Aspekte:

AppGuard läuft ohne Root-Rechte auf fast allen Geräten
Es schützt die sensiblen Daten der Nutzer
Einfache Bedienung mit „Aha-Faktor“ durch die Log-Funktion

Allerdings dürfen die negativen Aspekte nicht vergessen werden:

Verstößt gegen bestehende Nutzungsbedingungen von Apps. Der Quellcode wird nachträglich verändert. Vermutlich auch der Grund für den Ausschluss aus dem Google Play Store.
Apps werden modifiziert. Unter Umständen kann dies Fehlfunktionen hervorrufen. Außerdem muss AppGuard immer installiert bleiben. Ansonsten besteht auch bei modifizierten Apps kein Schutz. Durch die Modifikation der App verliert der User alle Einstellungen und zugehörigen Daten.
Fazit: Apps werden unrechtmäßig verändert und Apps werden durch die Blockierung der falschen Berechtigungen sogar unbrauchbar.

Die negativen Punkte stoßen insgesamt etwas säuerlich auf. Wer sich damit anfreunden kann findet mit AppGuard dennoch eine App, der es gelingt sensible Daten zu schützen. Man sollte sich aber mit den Berechtigungen von Apps auskennen, ansonsten werden Funktionen blockiert, die man eventuell braucht.

9.18 ChatSecure

ChatSecure ist ein Teil des Guardian Projects, das es sich zum Ziel gesetzt hat, mit einfach zu bedienenden Apps die Privatsphäre und Sicherheit seiner Nutzer zu schützen. Dabei ist ChatSecure für die verschlüsselte Kommunikation per Chat zuständig.

Bevor wir zur Installation übergehen, solltest du dir erst überlegen, welchen Jabber-Server du willst. Anders als proprietäre Messenger hat Jabber viele verschiedene Server. Die bekanntesten und meist genutzten sind der vom Chaos Computer Club (www.jabber.ccc.de) und der von Jabber.org (www.jabber.org).

Bei der Auswahl des Servers solltest du darauf achten, einen möglichst großen zu wählen und dass dieser SSL unterstützt. Bei kleineren ist die Chance groß, dass sie plötzlich einfach vom Netz gehen. Wir würden dir also empfehlen, den vom CCC oder jabber.org zu nehmen.

Für manche vieleicht interessant: deine Jabber-Adresse (Jabber ID = JID) wird wie eine eBrief Adresse aussehen, wobei der Server den letzten Teil darstellt. John-Doe@jabber.ccc.de wäre eine hypothetische Beispieladresse.

Du musst dir die neuste Version von ChatSecure im Google Play Store herunterladen und auf deinem Mobiltelefon installieren.

Unterstützt werden XMPP- und Jabber-Server, somit ist ChatSecure unter anderem auch mit Google Talk und dem Facebook-Chat kompatibel. Für die Verschlüsselung und Verifizierung deines Chatpartners kommt OTR zum Einsatz.

Optional kann via Orbot zusätzlich eine Verbindung über das Tor-Netzwerk hergestellt werden.

9.19 DuckDuckGo

Immer mehr Weltnetznutzer verwenden anstatt Google alternative, anonyme Suchmaschinen. Was jedoch die wenigsten wissen: Es gibt eine DuckDuckGo-App für Android.

Mittlerweile stehen viele Weltnetznutzer Google kritisch gegenüber und verwenden stattdessen alternative Suchmaschinen wie z.B. DuckDuckGo.com. So verzeichnete die anonyme Internetsuche aufgrund der Berichterstattungen in den letzten Wochen über diverse staatliche Schnüffelaktionen einen starken Zuwachs an Suchanfragen.

Nur wenige Anwender wissen aber, dass es von DuckDuckGo.com auch eine eigene Such-App für Android-Geräte gibt. Damit sucht man auch auf dem Smartphone oder Tablet bequem anonym im Weltnetz.

Die App DuckDuckGo Search & Stories für Android ab Version 2.2 gibt es im Google Play Store.

Vorteile von DuckDuckGo.com

Mit DuckDuckGo.com sucht man im Weltnetz ohne Spuren zu hinterlassen. Die Suchmaschine speichert keine Suchanfragen, IP-Adressen oder Cookies. DuckDuckGo.com übermittelt bei einem Klick auf ein Suchergebnis keinerlei Informationen an diese Weltnetzseite. Die Seite weiß also nicht einmal dass man von DuckDuckGo.com kommt.

Du kannst die App in den Einstellungen auch über Orbot laufen lassen. Dann suchst du anonym per Tor-Netzwerk.

9.20 Ich bekomme Arrested

Hier stellen wir dir eine Erweiterung (APP) für dein Mobiltelefon vor, die von Mitgliedern der Occupy Bewegung ausschießlich für Demonstrationen entworfen wurde. Wirst du während einer Demonstration von der Polizei verhaftet oder gerätst anderweitig in bedrängnis kannst du mit einem Klick eine Kurzmitteilung (SMS) an beliebig viele Kameraden schicken.

Es ist immer ratsam, falls vorhanden, auch dem für die Demonstration zuständigen EA eine Nachricht zukommen zu lassen.

Im Google Play Store herunterladen und installieren.
Hier trägst du die Kurznachricht und die Telefonnummern, jeweils mit einem Leerzeichen getrennt, ein.
Willst du die Notruf Kurzmitteilung verschicken, musst du wenige Sekunden auf den Button drücken.
Das einzige Manko an dieser Erweiterung ist, dass sie immer geöffnet sein muss um einen Notruf absetzen zu können.

9.21 K-9 Mail

Seit langer Zeit rangiert der eBrief-Client K-9 Mail ganz oben auf der Beliebtheitsskala mancher Android-Nutzer. Der Grund dafür liegt in erster Linie darin, dass die App extrem schnell arbeitet und mit praktisch allen eBrief-Konten klarkommt. K-9 beherrscht POP3, IMAP und Push-Mail, auch mit einem Exchange-Server lässt sich das Programm nutzen, allerdings nur über die Webdav-Schnittstelle, Active Sync unterstützt K-9 Mail nicht.

K-9 beherrscht Push-Mail, sofern das benutzte Konto Push unterstützt. Steht Push nicht zur Verfügung, erfolgt der Abruf der eBriefe wahlweise manuell oder in konfigurierbaren Zeitintervallen. Push funktioniert unter K-9 blitzschnell und zuverlässig. Löscht etwa der Nutzer eine Nachricht in Thunderbird am Computer, verschwindet sie binnen Sekunden auch auf dem Smartphone und umgekehrt. Allerdings läuft das automatische Synchronisieren auch schon mal ins Leere, falls der Nutzer häufig zwischen WLAN und UMTS/GPRS/EDGE wechselt. Im Übrigen ist das Synchronisieren eingehender Nachrichten auch im Hintergrund möglich.

Herausragend an K-9 sind die leistungsfähige Suchfunktion und die Ordnersynchronisation für IMAP. So kann der Nutzer etwa IMAP-Ordnern die Eigenschaft Haupt-Ordner oder Neben-Ordner zuweisen, bzw. mit Hilfe so genannter Synchronisations-Klassen und Push-Klassen festlegen, welche IMAP-Ordner K-9 in die Synchronisation einbezieht. Die Unterscheidung in Haupt- und Neben-Ordner bewirkt, dass K-9 wahlweise alle Ordner, nur die Haupt-Ordner oder nur die Neben-Ordner anzeigt. Die gleichen Optionen gibt es in der Liste beim Kopieren und Verschieben angezeigter Ordner. K-9 kennt allerdings nur einen Namensbereich. Damit funktioniert der Zugriff auf die in vielen Unternehmen gebräuchlichen gemeinsamen IMAP-Ordner nur dann, wenn der Nutzer nicht gleichzeitig private IMAP-Ordner verwendet.

Herunterladen kannst du den eBrief-Client K-9 Mail, wie immer im Google Play Store.
K-9 eBrief-Adresse einrichten

Die Einrichtung der eBriefadresse benötigt nur wenige Schritte. Gib im ersten Fenster deine eBrief-Adresse mit dem dazugehörigen Passwort ein.

Im nächsten Fenster gibst du optional einen Kontonamen an und als zweites den Namen der bei ausgehenden eBriefen Angezeigt wird.

Das war es schon. Jetzt hast du deine eBrief-Adresse eingerichtet und kannst eBriefe mit K-9 senden und empfangen.

K-9 praktisch
Das GUI orientiert sich bei K-9 weitgehend am Original von Google, weshalb K-9 unter Android-Nutzern auch als beste Alternative zu GMail gehandelt wird. Im Unterschied zum Standard-Mailer können K-9-Nutzer die Mail-Ansicht im Eingangsordner wahlweise zweizeilig oder dreizeilig einstellen. Im letzteren Modus zeigt die Liste jeweils die erste Zeile des Inhalts mit an. Außerdem kann der Anwender einzelne oder mehrere eBriefe markieren. Das Markieren einzelner eBriefe erfolgt über das Kontextmenü der Nachricht, wozu der Nutzer auf eine einzelne eBriefe drücken und den Druck eine zeitlang halten muss. Jetzt kann er im Kontextmenü den Eintrag Auswählen drücken, wodurch K-9 am unteren Bildrand die möglichen Optionen Posteingang abrufen , als gelesen/ungelesen kennzeichnen , löschen und mit einem Stern markieren anzeigt. Thunderbird und die meisten eBrief-Clients übernehmen die Stern-Kennzeichnung. Einfacher ist das Markieren sämtlicher eBriefe, wozu der Nutzer nur das Einstellungsmenü der App aufruft.

K-9 konfigurieren
Die wichtigste Einstellung für uns ist die Verschlüsselung der eBriefe. Im Menüpunkt „Kryptographie“ setzt du den „OpenPGP-Provider“ dann auf „APG“. Damit ist die Verschlüsselung nun

möglich.

K-9-Integration
Im Nachrichteneditor werden zwei neue Optionsboxen angezeigt, mit denen du das Unterzeichnen oder Verschlüsseln der aktuellen Nachricht aktivieren kannst. Wurde die Verschlüsselungsoption gesetzt, öffnet sich ein APG Fenster, in dem du den Public Key des Empfängers auswählst. Dafür muss der Public Key aber in APG Importiert worden sein. Das kann wie oben erklärt über die Importieren-Funktion von APG passieren oder über eine Suche auf den Keyservern, auf denen PGP Nutzer ihre Public Keys ablegen können.

9.22 KeePassDroid

Nachdem wir KeePass als quelloffene Passwortverwaltung für deinen Computer vorgestellt haben, folgt nun die App. Herunterladen kannst du diese wie immer im Google Play Store. Warum sollte man auch alle Passwörter im Mobiltelefon noch mal erneut speichern, wenn man die Datenbank des Desktop-Clients einfach übernehmen kann? „Nachteil“: Das Programm kann momentan nur mit den .kdb-Datenbanken von KeePass 1.x umgehen, die neue Version 2.x mit der Endung *.kdbx werden (noch) nicht unterstützt und das ist auch der Grund, warum ich auf dem Computer die Version 1.17 verwende. Funktional sehe ich aber dadurch keine Einschränkung.

Im Endeffekt funktioniert das Programm ganz einfach: Du exportierst deine Passwörter aus dem Desktop-Client über das Menü „Datei -¿ Export -¿ KeePass Datenbank“ und kopierst die .kdb-Datei auf die SD-Karte deines Android-Mobiltelefons. Nach Installation und Start von KeePass-Droid gibst du zuerst ein mal den Pfad zur KeePass Datenbank an und klickst auf Öffnen.

Solltest du mit einer neuen, leeren Datenbank beginnen wollen und nicht die Daten vom Computer übernehmen, erstellst du eben einfach auf dem gleichen Bildschirm eine neue Passwort-Datenbank.

Nach dem Öffnen der Datei wirst du nach deinem Passwort gefragt und musst, falls du das beim Desktop-Client auch so gemacht hast, deine Schlüsseldatei auswählen. Ich muss glaube ich nicht extra erwähnen, dass du immer auf sichere Passwörter achten solltest.

Im Endeffekt ist die Datenbank auf dem Telefon genauso aufgeteilt, wie im Desktop-Programm auch. Solltest du verschiedene Gruppen von Kennwörtern haben, beispielsweise Weltnetz, Online-Banking, eBrief, Netzwerk und Programme, werden genau diese Gruppen auch so im Mobiltelefon angezeigt. Ein Klick auf eine Gruppe öffnet diese, danach werden euch alle Einträge angezeigt, was dann in etwa so aussehen könnte:

Klickst du nun auf einen der Einträge, wird dieser geöffnet. Gleichzeitig hierzu werden oben in der Systemleiste zwei Einträge erstellt, nämlich „Copy username to clipboard“ und „Copy password to clipboard“. Du kannst jetzt auf die gewünschte Weltnetzseite wechseln, das entsprechende Programm starten usw., für welches du die Benutzerdaten brauchst. Dann wählst du beispielsweise zuerst den Eintrag Benutzername kopieren aus und fügst ihn durch einen langen Klick auf das Feld Benutzername auf der Weltnetzseite ein. Das gleiche machst du mit dem Passwort und schon hast du deine Anmeldedaten aus der Datenbank in die Weltnetzseite übernommen.

Über das Menü, welches du über die Menü-Taste aufrufen kannst, hast du noch ein paar Optionen, du kannst dort die Datenbank wieder sperren, damit z. B. wenn du das Mobiltelefon danach jemand anderem gibst, dieser nicht in deine Passwortliste sehen kann. Außerdem kannst du nach Einträgen suchen, solltest du mal vergessen haben, in welcher Gruppe ein bestimmter Datensatz gespeichert wurde. Du kannst das Programm über den Menüpunkt „Settings“ konfigurieren und das Datenbankpasswort ändern. Zu guter Letzt hast du dort noch die Möglichkeit, dem Entwickler über PayPal einen beliebigen Betrag zu spenden. Da das Programm, wie auch der Desktop-Client Open Source und damit kostenlos ist, freuen sich die Entwickler über jede noch so kleine Spende

und damit hält man solche Projekte auch am Laufen. Das muss allerdings jeder für sich selbst bestimmen, die Spende ist selbstverständlich absolut freiwillig.

9.23 Mozilla Firefox

Wie auch auf dem Desktop-Computer empfehlen wir dir auf deinem Smartphone die Verwendung vom Firefox Netzbetrachter. Die Android-Version des Netzbetrachters benutzt dieselbe Engine wie der „große Bruder“, kommt genau so mit Erweiterungen zurecht und ist in Sachen User-Interface komplett für die Bedürfnisse von Touchpads optimiert.

Herunterladen kannst du die Netzbetrachter-App wie immer im Google Play Store.

In Firefox für Android ist Firefox Sync integriert, mit dem du im Handumdrehen alle Einstellungen deines Desktop-Browsers inklusive Lesezeichen, Seitenverlauf, Tabs, Passwörter, Formulardaten und Erweiterungen in die mobile Version übernehmen kannst. Außerdem kannst du auch bequem Lesezeichen zu deinem Android-Startbildschirm hinzufügen. Die Weltnetzseiten lassen sich dann mit einem einzigen Klick direkt über den Startbildschirm aufrufen. Der Mozilla-Netzbetrachter erlaubt zudem privates „surfen“ für einzelne Tabs.

9.24 https Everywhere - Add-On

Die Eletronic Frontier Foundation (EFF) bietet ihre Browser-Extension HTTPS Everywhere seit kurzem in einer Beta-Version für Mozilla Firefox auf Android an.

In Zeiten, in denen auch die Geheimdienste sich für das Nutzungsverhalten von Smartphone-Besitzern interessieren ist dies zumindest ein kleiner Schritt für mehr Privatsphäre. Was man da unter anderem alles erschwert, hat Linus Neumann vor einiger Zeit hier beschrieben. Hundertprozentige Sicherheit ist damit natürlich noch nicht hergestellt, unter anderem, weil HTTPS Everywhere logischerweise auch nur dort für HTTPS-Verbindungen sorgen kann, wo diese unterstützt werden.

Das Vorgehen ist recht simpel: Einfach die aktuellste Version des Netzbetrachters Firefox installieren und den Download von HTTPS Everywhere starten.

Immer wenn du eine per HTTPS geschützte Weltnetzseite aufrufst erscheint das von uns im Bild markierte Symbol.

9.25 No Script - Add-On

Die kleine aber feine Erweiterung NoScript hat sich seit langem bewährt, wenn es darum geht, gefährliche JavaScripts zu stoppen. Jetzt steht endlich auch eine erste Alpha-Version des Sicherheits-Add-Ons für Firefox für Android zum Download bereit.

Nach der Installation erscheint das NoScript-Symbol rechts in der Adressleiste des Firefox. Von hier aus kannst du individuell für jede aufgerufene Seite Script-Berechtigungen festlegen. Über den Eintrag „Add-Ons“ hast du Zugriff auf weitere Features - wie beispielsweise den Cross-Site-Scripting-Filter sowie den Clickjacking-Schutz.

Das Vorgehen ist recht simpel: Einfach die aktuellste Version des Netzbetrachters Firefox installieren und den Download von NoScript starten.

9.26 Proxy Mobile - Add-On

Mit dem kostenlosen mobilen Firefox Add-On „Proxy Mobile“ surfst du dank Proxy-Server im Weltnetz, ohne deine Identität preiszugeben.

Der Entwickler des mobilen Firefox Add-ons „Proxy Mobile“ sagt Datendiebstahl den Kampf an. The Guardian Project hat sich zum Ziel gesetzt, den steigenden Verlust der Anonymität, Sicherheit und Privatsphäre von Smartphone-Nutzern zu beenden. Ein Ergebnis des Projekts ist „Proxy Mobile“.

Das Add-on, das zusätzlich zur Firefox Android App heruntergeladen wird, birgt die Möglichkeit, einen Proxy-Servern einzurichten, um somit für zusätzliche Sicherheit am Smartphone zu sorgen. Standardmäßig bedient sich „Proxy Mobile“ dabei an den Einstellungen des bekannten Verschlüsselungsprogramms Orbot, weswegen die Orbot-App installiert sein muss, um den Proxy-Server zu verwenden. Dieser steht im Übrigen in den USA, was den netten Nebeneffekt hat, dass du künftig in Europa gesperrte US-Webseiten aufrufen kannst.

Alternativ bist du die Host-Daten eines anderen Proxy-Servers ein. Wer also statt einer amerikanischen IP-Adresse lieber eine britische oder französische verwenden will, kann das ebenfalls. Im Proxy Server Artikel findest du Anonyme Proxy-Server Listen

Das Vorgehen ist recht simpel: Einfach die aktuellste Version des Netzbetrachters Firefox installieren und den Download von Proxy Mobile starten.

9.27 Ghostery - Add-On

Tracker sind leider in den seltensten Fällen so offensichtlich wie die „Gefällt mir“ Buttons. Am weitesten verbreitet ist „Google Analytics“, eine von Google bereitgestellte Software, welche zur Erstellung von Statistiken über die Nutzung einer Webseite dient. Bindet ein Betreiber diesen Dienst ein, werden die Daten zentral von Google erfasst und ausgewertet. Dadurch kann Google in Verbindung mit vielen anderen Quellen, Profile der Benutzer erstellen.

„Ghostery“ enthält eine Liste der gängigsten Tracker und wird ständig aktualisiert. Leider erfordert es ein kleines bisschen Konfiguration, dafür schützt es aber sehr zuverlässig vor den meisten Trackern.

Das Vorgehen ist recht simpel: Einfach die aktuellste Version des Netzbetrachters Firefox installieren und den Download von Ghostery starten. Extrem wichtig ist das du dieses Add-On wie in dem Netzbetrachter Add-On Leitfaden konfigurierst damit es dich wirkungsvoll vor Trackern schützen kann.

9.27.1 Note Cipher

Den meisten Nutzern dürfte bekannt sein, dass vertrauliche Informationen niemals ungeschützt auf dem Mobiltelefon angelegt werden sollten. Das kostenlose NoteCipher bietet dir die Möglichkeit, deine Notizen per passwortgeschützter 256-Bit-Verschlüsselung zu sichern.

Du kannst diese App im Google Play Store herunterladen. Nach der Installation des Open-Source-Tools musst du zunächst ein sicheres Passwort erstellen, das den unbefugten Zugriff auf den Notizblock verhindert.

Anschließend kannst du auch schon deine Notizen wie gewohnt anlegen.

9.28 ObscuraCam

ObscuraCam will den Datenschutz auf Fotos und Videos verbessern. In Zeiten automatischer Gesichtserkennung auf Facebook, Goolge Plus und Co. hilft dir die App dabei, Gesichter auf Fotos und in Videos unkenntlich zu machen.

Die Menschenrechtsorganisation WITNESS (witness.org) und die Sicherheitsexperten von The Guardian Project (guardianproject.info) haben eine neue Version der Android-App ObscuraCam veröffentlicht. Diese bringt nun Unterstützung für Videos mit und erlaubt die einfache Unkenntlichmachung der Gesichter gefilmter Personen. Das Tool soll unter anderem Aktivisten zugute kommen, deren Identifikation in ihren Heimatstaaten gefährliche Folgen für sie haben könnte.

Bislang konnte das auf dem „South by Southwest“-Festival vorgestellte Programm ausschließlich mit Fotos umgehen. Die Erweiterung auf bewegte Bilder ist jedoch nicht nur für Regimegegner in Syrien, Bahrain und anderen Staaten interessant, sondern auch für alle anderen Nutzer, die ihre Privatsphäre im Weltnetz gewahrt wissen möchten.

Du kannst diese App im Google Play Store herunterladen.

9.29 OpenVPN

Mit OpenVPN errichtest du ein virtuelles und verschlüsseltes Netzwerk. Herunterladen kannst du es im Google Play Store.

OpenVPN hilft dir beim Aufbau eines virtuellen Netzwerkes über eine verschlüsselte SSL-Verbindung. Das Programm greift dabei auf OpenSSL-Bibilotheken zurück. Die Software verwendet dafür wahlweise UDP oder TCP.

Für die Sicherheit stehen zwei Authentifizierungsarten zur Verfügung. Beim Benutzen eines „preshared key“ werden alle Daten mit dem selben Schlüssel ent- und verschlüsselt. Bei der zertifikatbasierten Authentifizierung werden Schlüsselpaare verwendet, die es möglich machen bestimmte Nutzer auszusperren.

Die exakte Funktionsweise von OpenVPN findest du auf der Wikipedia-Seite. Eine genaue Anleitung zur Installation und Nutzung gibt es auf der Hersteller-Weltnetzseite.

9.30 Orbot & Orfox

The Guardian Project, ein Ableger des Tor-Projekts, stellt für Android mit „Orbot“ einen Proxy-Client bereit der den Weltnetzverkehr über das anonyme Tor Netzwerk leiten kann. Ausserdem stellen sie mit „Orfox“ einen anonymen Netzbetrachter zur freien Verfügung, der via „Orbot“ auf das Proxy-Netzwerk von Tor zurückgreift. Das Tor-Netzwerk ist bekannt dafür, eine der sichersten Lösungen zu sein, wenn es darum geht, im Weltnetz anonym zu bleiben

Mit der „Orbot-Proxy-App“ in Kombination mit dem „Orfox Netzbetrachter“ erhalten Aktivisten eine absolut anonyme Möglichkeit sich mit dem Mobiltelefon im Weltnetz zu bewegen. Weder in deinem Netzwerk noch auf besuchten Weltnetzseiten wird deine echte IP-Adresse preisgegeben. Neben „Orbot“ unterstützt „Orfox“ aber auch die Weiterleitung über einen jeden anderen HTTP-Proxy. Mit „Orbot“ in Kombination mit „Orfox“ verleihst du deinem Androiden eine Tarnkappe. Sowohl deine Standort- und anderen Mobiltelefon-Daten als auch deine Weltnetzaktivitäten bleiben damit dein Geheimnis.

Lade dir die aktuellsten Versionen der Apps im Google Play Store herunter und installiere sie auf deinem Mobiltelefon.
Sind beide Applikationen heruntergeladen und installiert startest du Orbot das erste mal und siehst dieses Bild.

Um die Verbindung zum Tor-Netzwerk herzustellen drückst du 1-2 Sekunden auf die Zwiebel, den Einschalt-Button in der Mitte des Bildschirms. Es kann je nach Telefon und Weltnetzverbindung einige Sekunden dauern bis sich Orbot vollständig verbunden hat.

Willst du auf eine Weltnetzseite die nur von bestimmten Regionen der Welt besucht werden kann oder willst du dich, aus welchem Grund auch immer, nur über ein bestimmtes Land mit dem Weltnetz verbinden, so kannst du in der rechten- unteren Ecke per Klick auf das Pfeilsymbot ein Fenster öffnen in dem neben „World“ verschiedene Länder zur Auswahl angeboten werden. Klickst du hier z.B. auf „Germany“ werden deine Weltnetzanfragen ausschließlich über deutsche Tor-Server geleitet. Wir empfehlen dir in der Regel die Region „World“ aktiv zu lassen. Die Wahrscheinlichkeit enttarnt zu werden sinkt proportional zur Anzahl der aktiven Tor-Server mit denen du dich verbinden kannst

Hat sich „Orbot“ nun erfolgeich mit dem Tor Netzwerk verbunden ist es soweit das du die App „Orfox“ starten kannst. „Orfox“ ist eine modifizierte Version des normalen Firefox Netzbetrachters, du wirst dich sicher schnell zurecht finden. Öffnest du den Netzbetrachter findest du im ersten Schnellstartfester das Feld: „Check Tor Connection“. Mit einem Klick auf dieses Feld wirst du auf die Weltnetzseite des Tor-Projects geleitet und dort wirst du feststellen, dass du erfolgreich mit dem Tor-Netzwerk verbunden bist. Du kannst dich jetzt sicher über das Tor-Netzwerk im Weltnetz bewegen.

Nutze für deine Aktivitäten und Recherchen im Weltnetz ausschließlich „Orfox“! Dieser Netzbetrachter verbirgt immer deine IP-Adresse. Solltest du versuchen den „Orfox“ Netzbetrachter zu benutzen ohne vorher Örbotëingeschaltet zu haben wirst du keine Verbindung zum Weltnetz herstellen können

Tor-Identität
Um deine Spuren im Weltnetz noch besser zu verwischen, startest du „Orbot“ und streichst seitwärts über den aktivierten Zwiebel-Button. Er sollte sich nun um seine eigene Achse drehen. Dabei wandelt sich die Tor-Identität, wodurch sich deine IP-Adresse, mit der du dich im Netz bewegst, ändert.

Die App „Orbot“ startet standartmäßig mit dem Telefonstart und verbindet sich automatisch mit dem Tor-Netzwerk. Dies geschieht im Hintergrund. Du bemerkst es aber wenn in der Statusleiste deines Telefons das Onion Symbol auftaucht.

Wenn du dies nicht möchtest musst du in der App rechts oben auf das Schraubenschlüssel-Symbol klicken und im sich öffnenden Fenster, den Haken bei Start Orbot on Boot herausnehmen.
Viele nationale Aktivisten nutzen inzwischen Twitter. Vergesst bitte nicht dieses Netzwerk ausschließlich über eine sichere Verbindung zu besuchen. Mehr informationen zum sicheren Umgang mit der Twitter App erhälst du im: SfN Infoblog

9.31 Passwort-Generator

Diese Erweiterung für dein Mobiltelefon bedarf nicht vieler Worte. Im Google Play Store herunterladen, installieren und deine neuen Passwörter erstellen. Informationen zur Wahl eines guten Passworts findest du im Artikel: Passwortwahl.

9.32 Signal und Conversations - „Sichere“ Messenger

Spätestens seit dem Spionageskandal wollen mehr und mehr Aktivisten ihre Privatsphäre verstärkt schützen. Dabei führt fast kein Weg an einer Verschlüsselung der eigenen Kommunikation vorbei. Wer nicht nur daran denkt seine eBriefe zu verschlüsseln, sondern auch die privaten Chat- und Gruppengespräche sowie seine SMS und Telefongespräche sichern möchte, findet in der App „Signal - Sicherer Messenger“ einen sehr starken Partner[3].

„Open Whisper Systems“ hat die lange angekündigte Vereinigung seiner beiden Android-Apps TextSecure und RedPhone vollzogen. Beide Apps wurden nun unter dem Namen Signal kombiniert und bieten Ende-zu-Ende verschlüsselte Chats und Telefonate an - genau wie Signal auf iOS das schon seit Anfang des Jahres tut. „Open Whisper Systems“ st eine App-Entwicklergruppe hinter welcher unter anderem Moxie Marlinspike steckt, ein nicht ganz unbekannter Name in der Hacker-Szene.

Herunterladen kannst du dir die benötigte App wie immer im Google Play Store. Zum Austausch verschlüsselter Nachrichten und Anrufe müssen sowohl Sender als auch Empfänger die App auf dem Smartphone installiert haben

Ist die App installiert musst du dich mit dem Signal Server verbinden, das heißt du gibst einfach deine Telefonnummer (mit Landesvorwahl) an und registrierst dich bei dem Dienst. Im nächsten Schritt wird der Sicherheitsschlüssel erstellt und die Telefonnummer durch eine SMS mit einem Code überprüft. Signal sollte die SMS automatisch erkennen und sich selbständig für den Betrieb freischalten.

Signal ist jetzt fertig installiert, kommen wir zu den Einstellungen. Die App möchte das du sie als Standart-SMS-App verwendest. Es gibt Stimmen die dies kritisch sehen jedoch sehen wir mehr Vorteile als Nachteile. Deswegen klicken wir auf das blaue Schriftfeld.

Du solltest deine Standart-SMS-App durch Signal ersetzen! Signal ermöglicht es reibungslos verschlüsselte und unverschlüsselte Chats/SMS nebeneinander laufen zu lassen. Dabei lässt sich durch die Farbkodierung jeder Zeit erkennen, ob man eine unsichere SMS oder eine mit dem Whisper-Systems-Protokoll verschlüsselte Nachricht versendet.

Als nächstes kannst du entscheiden, ob deine vorhandenen SMS-Nachrichten in die verschlüsselte Datenbank aufgenommen werden sollen.

Die bisher geschriebenen SMS sind nach dem Klick auf das Feld trotzdem noch im Standard-SMS-Programm deines Smartphones gespeichert und müssen dort manuell gelöscht werden. Alle ab jetzt hinzukommenden SMS werden aber im Datentresor abgelegt.

Du kannst Signal jetzt für den Versand der sicheren Nachrichten, SMS und die sichere Telefonie nutzen. Da wir aber nicht wollen das jeder x-Beliebige der unser Telefon in die Hand bekommt diese Nachrichten lesen kann gehen wir in die „Einstellungen“ der App und zu dem Reiter „Datenschutz“. Dort aktivieren wir den Schutz der App indem wir ein Passwort eingeben, welches recht stark sein sollte und mit welchem anschließend die App gesperrt und deine Nachrichten auf dem Gerät verschlüsselt werden.

Da immer wieder vergessen wird die App manuell zu sperren haben die Entwickler den Punkt „Passwort bei Inaktivität“ eingebaut. Diesen sollte man auf jedenfall mit einem Haken versehen und die Verzögerungszeit auf 1 - 5 Minuten stellen.

[3] die App „Conversations“ soll noch besser als Signal sein

Du musst jetzt bei jedem öffnen der App dein Passwort eingeben

Sicherer Nachrichtenversand und SMS/MMS

Nach der Einrichtung der App kannst du ganz normal Nachrichten an deine Kontakte verschicken. Nachrichten an Kontakte welche kein Signal benutzen werden dabei unverschlüsselt, per SMS versendet.

Benutzt ein Kontakt jedoch auch Signal, so wird dir dies über ein entsprechendes Benachrichtungsfenster mitgeteilt. Anschließend startet eine Secure Session. Nun werden deine Nachrichten mit dem ausgewählten Kontakt nur noch als verschlüsselte Direktnachicht im Stil von WhatsApp ausgetauscht. Alle Konversationen werden auch auf dem Gerät verschlüsselt.

Eine neue Konversation lässt sich genau so einfach wie eine WhatsApp Unterhaltung erstellen, da die Bedienung nahezu identisch ist. So findest du in der Übersicht deiner Konversationen in der Bedienleiste am unteren Bildschirmrand die Button zum Erstellen einer neuen Nachricht.
VoIP Telefonate
Nochmal, damit du verschlüsselt mit deinem Gesprächspartner über das Android-Gerät telfonieren kannst, muss dieser ebenfalls die Anwendung nutzen

Wenn du nun einen Bekannten über die App anrufst, erscheint bei ihm der eingehende Anruf als Signal-Anruf. Daraufhin läuft die Verschlüsselung des Gesprächs in Echtzeit.

Ein verschlüsseltes Gespräch funktioniert mit der Anwendung nicht über den Mobilfunk, sprich GSM. Signal baut dafür extra eine VoIP-Verbindung auf, mit der du über das Weltnetz kommunizierst. Im heimischen WLAN-Netz telefonierst du somit kostenfrei und sicher. Unterwegs funktioniert das Telefonat über das 3G-Netz, wobei es zu Abstürzen kommen kann, wenn die Empfangsleistung ungenügend ist. Außerdem solltest du hierbei über eine Weltnetz-Flatrate verfügen, sonst steigen die Kosten ins Unermessliche.

Bei einer beidseitigen WLAN-Verbindung ist der Klang recht gut. Zwar kommt das gesprochene Wort knapp einige Sekunden verzögert beim Gesprächspartner an, dafür kann keine fremde Person mithören. Unterwegs ist über 3G der Ton erstaunlich klar und deutlich. Bei einem 30-sekündigen Kurzanruf lag der Datenverbrauch bei 1 MB. Telefonierest du nicht zu lange, geht das noch in Ordnung. Unsere klare Sicherheitsempfehlung gilt der Messenger App SIGNAL jedoch findest du im SfN Informationsblog unter dem Stichpunkt www.blog.s-f-n.org/tag/messenger weitere Artikel über WhatsApp, Threema, Telegram und co. ...

9.33 Verschlüssel dein Android-Smartphone

Die wichtigste Sicherheitsmaßnahme auf deinem Android-Smartphone ist, es zu verschlüsseln und „Automatisch sperren“ zu aktivieren.

Genau wie dein Computer enthält ein Smartphone eine unglaublich hohe Anzahl an sensiblen Daten die vor Fremdzugriff geschützt werden sollten. Wenn du dein Mobiltelefon verlierst, kann jemand, der es findet, auf die im Smartphone gespeicherten Daten zugreifen: Bilder, Adressen, Notizen. Ein erster Schutz ist PIN oder Passwort, aber das hilft nur unzureichend. Ist hingegen das komplette System verschlüsselt, kann es erst nach Eingabe eines Passwortes starten. Weil alle deine persönlichen Daten, deine eBriefe, dein Netzbetrachter, deine Apps und die Daten darin nicht lesbar sind, hat ein Dieb oder Finder keinen Zugriff auf diese Daten, ergo keine Chance für Identitätsdiebstahl oder Datenklau.

Ein verschlüsseltes Smartphone besteht eigentlich nur noch aus Hardware - jedenfalls für den neuen Besitzer ohne Passwort. Schlimm genug, dass das Gerät weg ist - aber wenigstens sind deine

Daten gegen Zugriffe geschützt. Verschlüsselung schützt dich in Grenzen auch gegen Manipulation, also dagegen, dass jemand allzu leicht auf deinem Telefon eine Spionage-App installieren kann. Das alles gilt natürlich nur, wenn niemand dein Passwort kennt.

Vorbereitung
Wichtig ist, die Verschlüsselung nicht erst im Urlaub zu starten, sondern schon Zuhause:

Lade den Akku voll auf.
Lasse das Gerät am Ladegerät.
Starte unbedingt neu, damit möglichst wenig Mist parallel läuft.
Rechne mit einer Stunde (!) Arbeitszeit, oder besser: Wartezeit.

Passwort einrichten
Zuallererst ist es wie mit jeder Verschlüsselung - Du brauchst (sinnvollerweise) ein starkes Passwort mit dem du deine Verschlüsselung nutzen kannst.

Öffne zur Einrichtung eines Passwortes die Einstellungen deines Android-Geräts, klicke dort auf den Reiter Gerät und wähle Sperrbildschirm.

Wähle als Verfahren Passwort (hohe Sicherheit), nicht PIN. Eine PIN ist zu simpel für wirksamen Schutz!

Beachte bei der Wahl des Passwortes die Hinweise für sichere Passwörter.
Nehme nicht einfach ein Wort oder einen Namen, sonst können dich Freunde, Verwandte oder Kollegen durch einfaches raten „hacken“. Wähle also dein Passwort und bestätige die Eingabe.
Mache es dir aber auch nicht unnötig kompliziert, denn du musst das Kennwort dauernd eingeben; das wird dich ermüden und zermürben ...

Android verschlüsseln
Vergewissere dich nochmal, dass dein Gerät geladen und an den Strom angeschlossen ist. Starte das Gerät neu. Vergewissere dich durch den Neustart nochmal, dass dein Passwort auch wirklich funktioniert. Dann gehts los.

Öffne die Einstellungen deines Android-Geräts, klicke dort auf den Reiter Allgemein. Etwas herunterscrollen und Sicherheit wählen. Tippe in diesem Fenster im Bereich Verschlüsselung auf Gerät verschlüsseln. Wie du siehst gibt es keine weiteren Einstellungen zu tätigen. Bestätige den Sicherheitshinweis und klicke auf Gerät verschlüsseln.

Wenn dieser Menüpunkt nicht zu sehen ist, unterstützt das Gerät die Verschlüsselung nicht. Aber immerhin hast du es nun wenigstens mit einem Passwort gesichert

Hier gibst du das von dir gewählte, sichere Passwort einmal ein und bestätigst mit Weiter

Diese Hinweise stehen dort nicht umsonst. Achte darauf, dass das Telefon an das Ladekabel angeschlossen ist und lasse es die Stunde einfach Arbeiten. Mit einem Klick auf Gerät verschlüsseln aktivierst du die Verschlüsselung. Die schnelle Verschlüsselung ist von uns nicht zu beachten denn wir wollen das ganze Telefon verschlüsseln und nicht nur den Teil auf dem die Daten gelagert sind

Dann geht es los. Nach einiger Zeit (eine Stunde dauert es selten) ist das Gerät durch.

Ist die Verschlüssung abgeschlossen startet dein Telefon automatisch neu und fragt nach deinem Passwort. Es bootet künftig erst nach dessen Eingabe und auch danach kannst du erst nach dem Passwort auf dein Android-Gerät zugreifen. Das gilt auch für den Anschluss per USB. Wenn du

das Gerät an den Computer anschließt, kannst du erst dann über den Computer auf den Android-Speicher zugreifen, nachdem du am Android-Gerät das Passwort eingegeben hast.

9.34 Sicherheitsrisiko für Mobiltelefone: Öffentliche Ladestationen

Smartphones sind unsere täglichen kleinen Begleiter. Mit ihnen lassen sich Gespräche führen, wichtige eBriefe lesen und senden und im Weltnetz recherchieren.

Doch eine Schwäche haben die kleinen Alleskönner: Sie verbrauchen viel Energie und die Akkulaufzeit ist stark begrenzt. Natürlich macht der Akku gerade dann schlapp, wenn man unterwegs ist und das Ladekabel vergessen hat.

Rettung naht in solchen Fällen in Form von öffentliche Ladestationen. Diese lassen sich oft an Flughäfen finden. Sie halten Ladekabel für alle gängigen Mobiltelefone bereit. So kann man die lästige Wartezeit am Gate sinnvoll nutzen, um seinen treuen Begleiter aufzuladen. Endlich mal eine sinnvolle Erfindung, werden viele gedacht haben. Aber die Tankstellen für das Mobiltelefon birgen ein Sicherheitsrisiko für Daten auf dem Smartphone in sich.

Schon mal eine solche Station genutzt? Irgendwelche Bedenken gehabt? Fast alle Smartphones lassen sich über USB-Kabel laden. Diese Kabel eignen sich nicht nur zur Stromversorgung, sondern auch zum Datentransfer. Wird das Smartphone über den USB-Port eines PC geladen, wird in den meisten Fällen automatisch der Inhalt des Mobiltelefons angezeigt. Es ist somit relativ einfach, beim Aufladen Daten unbemerkt vom Smartphone zu kopieren.

Forscher haben dies auf einer Messe für Hacker ausprobiert. In weniger als vier Stunden hatten sich 360 Personen an die manipulierten Ladestationen angestöpselt. Diese Methode des Hackens wird Juice Jacking genannt.

Wissenschaftler sind bereits noch einen Schritt weiter. Wird ein Mobiltelefon an die manipulierte Ladestation angeschlossen und während des Ladevorgangs genutzt, spielt sich innerhalb von 60 Sekunden unbemerkt Malware auf das Smartphone. Eine bereits installierte App wird dabei durch eine manipulierte ersetzt. Für den Nutzer ist dieser Vorgang nicht zu bemerken. Nach erfolgter Installation werden alle Daten, auch die neu hinzugefügten, unbemerkt durch das Smartphone weitergeleitet. Von eBriefen über SMS bis zu Telefonbucheinträgen, nichts bleibt geheim.

Die Gefahr ist nicht ersichtlich, da sie am anderen Ende des Kabels schlummert. Es ist nicht erkennbar, ob die Anschlüsse manipuliert worden sind. Aus diesem Grund hilft auch das eigene Ladekabel nicht, wenn es an einen unbekannten USB-Port angeschlossen wird.

Vor dem nächsten Aufladen solltest du daher genau abwägen, ob du nicht ein paar Stunden auf die Erreichbarkeit verzichten kannst und dadurch aber deine Daten schützt. Ist man unterwegs auf eine Lademöglichkeit angewiesen, sollte man immer sein eigenes Ladegerät nutzen. Dies aber möglichst nicht an fremde USB-Anschlüsse schließen, sondern direkt an eine Steckdose.

Zusätzliche Sicherheit erhält man durch den Einsatz von sogenannten Charge Only Kabeln, die einen Datentransfer nicht unterstützen. Eine weitere Alternative ist ein Zusatzakku.

9.35 Root?!

Jeder, der ein Android-Smartphone besitzt und sich ein bisschen mit dem Gerät auseinandergesetzt hat, wird schon mal über den Begriff Root gestolpert sein. Da dies für viele Nutzer allerdings ein Buch mit 7 Siegeln ist, wollen wir in diesem Artikel erklären was Root ist und was man damit

eigentlich anfangen kann.

Was ist Root?
Ein Android-Gerät zu rooten oder Rootzugang zu erlangen bedeutet, das Betriebssystem dahingehend zu modifizieren, um komplette Kontrolle darüber zu erlangen. Somit lassen sich Beschränkungen, die der jeweilige Hersteller oder Mobilfunkanbieter auf dem Gerät eingebaut haben, umgehen.

Zunächst müssen wir ein beliebtes Missverständnis aus dem Weg räumen: Rooten ist nicht mit der Installation einer Custom ROM gleichzusetzen - dabei handelt es sich um eine modifizierte Variante des Betriebssystems; das auf dem Gerät befindliche OS wird durch den Root-Vorgang nicht verändert oder gelöscht.

Der Begriff Root kommt vom Open Source-Betriebssystem Linux, auf dem auch Android basiert. Root ist mit dem Administrator auf Windows-Rechnern vergleichbar - der Nutzer, der alle Privilegien auf dem System besitzt, wird unter Linux Root genannt.

Ein Android-Gerät zu rooten ist meistens sehr einfach - da der Vorgang allerdings von Gerät zu Gerät sehr unterschiedlich sein kann, werden wir hier keine Anleitung bereitstellen, sondern verweisen auf unsere bereits vorhandenen Anleitungen oder auf Google, wo sich unter dem Suchbegriff „(Name des Gerätes) root“ normalerweise eine vielzahl Anleitungen finden lassen. Die meisten Root-Vorgänge beinhalten die App SuperUser, mit deren Hilfe einzelnen Apps bei der Ausführung Root Rechte gewährt werden können.

Natürlich muss an dieser Stelle die obligatorische Warnung ausgesprochen werden, dass durch das Rooten die Garantie des Gerätes verfällt und bei unvorsichtigem Vorgehen oder die falsche Verwendung von zum Beispiel Overclock Apps, mit deren Hilfe der Prozessor des Gerätes übertaktet werden kann, Schäden am Gerät entstehen können. Im schlimmsten Fall wird das Gerät dadurch gebrickt, also zu einem nutzlosen Ziegelstein gemacht, der maximal als teurer Briefbeschwerer nützlich ist. Rooten geschieht also auf eigene Gefahr.

Vorteile von Root
Ein gerootetes Android-Gerät bietet eine vielzahl Vorteile; dazu gehören unter anderem:

- Volle Kontrolle über Android

  Nachdem ein Android-Gerät gerootet ist, kann man nicht nur dessen Boot Image austauschen, sondern auch dessen Systemdateien verändert sowie lästige System-Apps oder Anwendungen, die der Gerätehersteller netterweise integriert hat deinstallieren. Für dieses Vorgehen gibt es viele Methoden, eine der einfachsten und umfangreichsten ist allerdings Titanium Backup, das, wie der Name erahnen lässt, noch ein paar weitere Funktionen bietet.

- App-Daten sichern
  Mit dem bereits erwähnten Titanium Backup, einer App-basierten Backup-Lösung, lassen sich nicht nur System-Apps einfrieren oder gar deinstallieren, man kann natürlich auch die installierten Apps mitsamt Daten sichern. Diese können entweder auf der SD-Karte des Gerätes abgelegt werden oder bei diversen Cloud-Speicherdiensten wie Box oder Dropbox zwischengelagert werden. Zwar gibt es auch für nicht gerootete Geräte mit Helium (vormals Carbon) die Möglichkeit die App-Daten zu sichern, allerdings ist die App nicht annähernd so umfangreich und flexibel auf die Nutzerwünsche einstellbar, wie Titanium Backup.

- Nandroid Backup
  Ein NAND Backup bezeichnet eine Art der Datensicherung, bei der ein Abbild des kompletten Systems erstellt wird. Dies ist sicherlich eine der sinnvollsten Funktionen, die unter

Android durch Root ermöglicht werden. Somit ist es zum Beispiel möglich Custom ROMs auszuprobieren und immer wieder zum vorherigen System zurückkehren zu können. Um ein Nandroid Backup zu erstellen, wird allerdings ein Custom Recovery, wie zum Beispiel das ClockworkMod Recovery, benötigt. Es gibt viele Wege auf denen sich solch ein Custom Recovery installiert werden kann - die einfachste und vor allem für die meisten Geräte universell gültige Methode dürfte dabei allerdings die App ROM Manager darstellen. Nach der Installation der App und dem Gewähren der Superuser-Rechte muss das gewünschte Recovery ausgewählt und installiert werden, was im ROM Manager gleich die erste Option erledigt. Danach kann man entweder direkt über den ROM Manager Backups erstellen oder wiederherstellen oder man bootet das Gerät direkt ins Recovery und führt die Schritte manuell aus.

- Spezielle Root Apps
  Neben Anwendungen wie dem ROM Manager oder Titanium Backup, die wir bereits erwähnt haben, gibt es eine unüberschaubare Zahl spezieller Apps, die Root-Zugang benötigen. Mit dem Root Explorer kann man auf Dateien im System-Bereich zugreifen, JuiceDefender ermöglicht es dir, viele Einstellungen des Gerätes zu verändern um Energie zu sparen. Mit dem Move2SD Enabler lassen sich dagegen nahezu alle Apps auf die SD-Karte verschieben, um den internen Speicher zu entlasten.

- Droidwall ist eine Firewall die als Frontend für den bekannten Paketfilter iptables dient. Die App blockiert einzelnen Anwendungen den Zugriff auf das Datennetzwerk (2G/3G und/oder Wi-Fi). Damit können Anwendungen die absolut nichts im Weltnetz zu suchen haben vom „nach Hause telefonieren“ abgehalten werden. Orbot funktioniert zwar auch grundsätzlich ohne Root-Rechte. Möchtest du aber den gesamten Datenverkehr schützen, kommst du um die erweiterten Rechte nicht herum. Denn sonst kannst du nur wenige Apps nutzen, die Orbot unterstützen - immerhin gehören Twitter und Firefox dazu. Android hinterlässt oftmals überflüssige Dateien auf deinem Telefon. Zum Beispiel werden nicht wirklich alle Dateien gelöscht, falls du eine App deinstallierst. Mit der App SD Maid kannst du dein Smartphone von diesen überflüsseigen Dateien säubern.

Dies sind nur wenige Beispiele und die Liste könnte endlos weitergeführt werden, würde allerdings den Rahmen dieses Artikels um ein Vielfaches sprengen.
Flashen von Custom ROMs
Custom ROMs sind modifizierte oder komplett selbst kompilierte Android-Versionen, die den Funktionsumfang des Gerätes drastisch erhöhen können. Ein Custom ROM geht weit über einfache Veränderungen hinaus und kann einem Gerät ein komplett neuen Look verpassen und dafür sorgen, dass es sich wie ein neues Gerät anfühlt - zumindest Software-seitig.

Da es für jedes Gerät eine schiere Flut verschiedener Custom ROMs gibt, bleibt uns aufgrund von Platzmangel auch an dieser Stelle wieder nur der Verweis auf eine Suchmaschine deiner Wahl übrig. Bevor man ein neues Betriebssystem installiert, was entweder über den ROM Manager oder für erfahrenere Nutzer auch über Custom Recoverys geschieht, sollte man natürlich ein Nandroid Backup anlegen um jederzeit wieder zur Ausgangssituation zurückkehren zu können.

10 Selbstverteidigung

Selbstschutz und Selbstverteidigung - viele politische Aktivisten überlegen sich, wie sie ihre eigene Gesundheit schützen können. Leider hören wir immer wieder von brutalen Übergriffen der Antifa auf nationale Infostände oder auf Aktivisten die einfach nur arglos unterwegs sind. Aber auch Sicherheit für die Tochter oder die Frau sind ein wichtiges Thema. Jeder Aktivisten sollte, um sich bei einem linkskriminellen Angriff verteidigen zu können, zumindest die Grundtechniken einer beliebigen Kampfsportart erlernen. Noch gibt es aber auch sogenannte „legale Waffen“ die wir nutzen können um Angriffe abzuwehren. In dieser Übersicht haben wir legalen Waffen welche zur

Verteidigung erhältlich sind zusammengestellt. Desweiteren erklären wir worauf geachtet werden muss und was bei einem Angriff wirklich hilft.

Allerdings sind nicht alle Verteidigungsmittel gleich sinnvoll und vor allem sind gar nicht alle Verteidigungsmittel auch „legal“ und „legal in der Öffentlichkeit“. Jeder Waffenladen will letzten Endes etwas verkaufen und wird darum primär die nötigen Gesetze die den Verkauf bzw. den Kauf betreffen beachten. Eine rechtliche Beratung des Kunden findet in den meisten Fällen wohl erst auf Nachfrage statt.

Rechtliche Bewertung
Richtig ist, dass man für den Erwerb der meisten Verteidigungsmittel mindestens 18 Jahre sein muss. Dies berechtigt zwar zum Kauf einer „legalen Waffe“, bedeutet aber nicht, dass man nun auch damit in der Öffentlichkeit rumlaufen darf. Unabhängig von den rechtlichen Vorraussetzungen zum Führen einer Waffe zur Verteidigung, sollte man sich natürlich mit dem Notwehrrecht beschäftigen. Das bedeutet, nicht nur den Notwehr-Paragraphen (§32 StGB) lesen sondern ihn auch verstehen! Das Waffengesetz (WaffG) definiert „führen“ als das zugriffsbereite Mitführen einer Waffe. Dazu gehört also z.B. das Messer in der Hosentasche.

Taktischer Nutzen
Alle Mittel haben verschiedene Einsatzgrundsätze und Eigenschaften. Nicht jedes Mittel ist immer das Richtige. Außerdem muss der Einsatz mit der jeweiligen Waffe geübt werden! Ein Pfefferspray in den Tiefen der Handtasche nützt nichts. Ein Kubotan den ich mit führe aber nicht geübt habe ihn (unter Stress oder Angriffsdruck) zu benutzen nützt nichts. Eine Schreckschusspistole die ich erst aus einem Holster ziehen muss kostet viel Zeit und bei einem Gegner direkt vor mir ... nützt sie nichts.

CS-Gas
Bei 20% aller Menschen wirkt das Gas nicht, sie sind immun.
Elektroschocker
Wirkt nur im Nahkampf, welcher nicht empfohlen wird. Die Bedienung ist im Ernstfall zu kompliziert.
Schreckschuss- Gaspistolen
Abschreckungswirkung ist relativ groß, kann viele Schüsse in geringer Zeit abfeuern aber benötigt den kl. Waffenschein.
Jet Protector
Abwehrsystem auf Basis von Pfefferspray mit hoher Reichweite und hohem Druck.
Kubotan / Tacticalpen
Ein harter, kurzer „Stock“ zur Selbstverteidigung mittels Stößen gegen den Angreifer.
Pfefferspray
Idealer Selbstschutz, schnelle Wirkung, einfach Handhabung, günstige Preise.
Schlagstock
Unhandlich, schwer handzuhaben und eine Gefahr für das Opfer.
Schrillalarm
Erzeugt einen Ton so laut wie ein Düsenflugzeug beim Start. Geeignet als Ergänzung.
Selbstverteidigungsschirm
Die Funktionen eines echten Regenschirmes, aber erhöhte Stabilität als Abwehrwaffe.
Taktische Taschenlampe
Kann den Angreifer stark blenden und als Schlagwaffe benutzt werden.

10.1 CS-Gas

CS-Gas - oder auch Tränengas - wird in kleinen Spraydosen verkauft, genauso wie Pfefferspray. Der chemische Wirkstoff soll menschliche Angreifer abwehren.

Früher, bevor Pfefferspray entwickelt wurde, war Tränengas das Einsatzmittel von Sicherheitskräften weltweit. Auch heute wird es noch bei Demonstrationen gegen Aktivisten eingesetzt. Trotzdem wurde es insgesamt von Pfefferspray verdrängt.

Die Wirkung
Tränengas wirkt auf die Atemorgane und löst eine Reizung aus. Es ist sehr aggressiv und kann zu Verätzungen führen und gerade für Menschen mit Leberproblemen oder Asthmatikern ist Tränengas sehr gefährlich. Bis zu 20% der Menschen sind jedoch immun gegen CS-Gas, weswegen dann keine oder nur eine geringe Reizung auftritt. Bei Pfefferspray liegt diese Quote nur bei 2%. Bei Hunden ist Tränengas wenig wirksam, weil höhere Konzentrationen benötigt werden.

Verwendung
Tränengas wird in Spraydosen und in Schreckschusspistolen verwendet. Getroffen werden müssen die Atemorgane des Angreifers. Grundsätzliches zur Selbstverteidigung mit Sprays:

Niemals ankündigen, das man Reizgas anwenden wird. Der Gegner wird vorbereitet sein, die Augen schließen und die Luft anhalten, wenn er euch angreift. Das Gas immer überraschend einsetzen, im besten Fall, wenn der Gegner ausgeatmet hat - beobachtet den Brustkorb ! Rechtliches
CS-Gas ist frei verkäuflich an Menschen ab 14 Jahren.

Fazit
CS-Gas wirkt seltener, schwächer und unzuverlässiger als andere Abwehrmittel wie z.B. Pfefferspray. Nicht umsonst wird auch die Polizei heute nicht mehr mit CS-Gas ausgerüstet sondern das wirksamere Pfefferspray genutzt.

10.2 Elektroschocker

Ein Elektroschocker ist ein handliches Gerät, welches mit einem oder mehreren 9-Volt-Blöcken arbeitet. Das Gerät gibt bei Auslösung einen Stromimpuls mit einer sehr hohen Spannung ab (Elektroimpulsgeber), was Angreifer außer Gefecht setzen soll. Um diese Waffe zu Führen muss ein Prüfsigel vorliegen und man muss 18 Jahre alt sein

Der live-Test eines Fernsehsenders brachte es ans Tageslicht. Elktroschocker sind zur Selbstverteidigung nicht geeignet. Die Geräte wirken nur im Nahkampf, denn es muss ein direkter Kontakt zwischen Elektroschocker und Angreifer bestehen. Um Die Wirkung voll entfalten zu können, muss der Kontakt zwischen Angreifer und Elektroschocker gehalten werden (1-5 Sekunden)! Zuckt der Angreifer nach dem ersten Kontakt also schnell zurück, hat er zwar einen kurzen Schmerz verspürt, ist aber nicht außer Gefecht. Außerdem kann dicke Kleidung ebenso wie Alkohol, Drogen und Adrenalin die Wirkung massiv abschwächen.

Das ist gerade für Frauen (aber nicht nur) absolut ungeeignet. Wenn der Angreifer körperlich überlegen ist, kann das Opfer den Schocker entweder gar nicht zur Anwendung bringen oder das Gerät wird sogar gegen das Opfer selbst eingesetzt.

Rechtliches
Elektroschocker müssen ein amtliches unbedenklichkeits-Prüfsiegel aufweisen (PTB - Physikalischen Technischen Prüfanstalt). Sie sind an Personen über 18 Jahren frei verkäuflich. Die sogenannten „Taser“, also Elektroschocker die auf Distanz wirken, sind seit dem 01. April 2008 generell verboten und dürfen nicht mehr verkauft oder geführt werden.

Problem Handhabung
Ein Problem ist auch die Handhabung an sich. Meist besitzen die Geräte eine Sicherung, welche

zunächst deaktiviert werden muss. Anschließend muss noch die Auslösung bedient werden - dass alles kann im Eifer des Gefechts schon viel zu kompliziert sein.
Problem Batterie
Die Batterien im Schocker können sich entladen, wenn sie nicht regelmäßig überprüft werden. Dann ist das Gerät im Einsatzfall wirkungslos.
Fazit
Zum Zwecke der Selbstverteidigung sind Elektroschocker nur für Profis geeignet. Die Handhabung ist zu kompliziert, die Wahrscheinlichkeit einer erfolgreichen Abwehr zu gering und die Gefahr der Anwendung gegen das Opfer selbst bzw. die Gefahr, dass die Geräte nicht funktionieren zu hoch.

10.3 Schreckschuss- Gaspistolen

Legale Schreckschusswaffen müssen über ein PTB Siegel der Physikalischen Technischen Prüfanstalt verfügen. Ab 18 Jahren kann man sie kaufen und auch auf seinem Privatgelände führen. Für das Führen in der Öffentlichkeit, benötigt man aber einen kleinen Waffenschein.

Schreckschuss- Gaspistolen sind Abwehrmittel, die das Aussehen einer Schusswaffe haben. Bei Auslösung wird mit der passenden Munition ein Gasgemisch abgegeben. Im Regelfall handelt es sich um CS-Tränengas bzw. Pfeffergas. Die Reichweite von 9mm-Pfeffermunition ist größer als bei den meisten Pfeffersprays. Auch sind nicht alle Sprays zuverlässig, d.h. mehr als einmal sprühen (3-4 Sek.) ist meist nicht möglich. Eine Schreckschusspistole wird jedoch mit mehreren Patronen geladen. Anschließend kann durch Auslösung mehrmals ein Gasgemisch abgegeben werden. Das CS-Tränengas bzw. Pfeffer-Gas soll den Angreifer in die Flucht schlagen.

Das Problem liegt in der Handhabung. Im Ernstfall kann die „Waffe“ sehr leicht gegen das Opfer verwendet werden. Bei Auslösung nahe am Körper entsteht ein großer Druck, was zu schweren Verletzungen der Haut führen kann deshalb halte immer genügend abstand zu dem Angreifer.

Wenn man nicht erst droht und „Cowboy spielt“ kann man eine Schreckschusspistole genauso unvermittelt einsetzen wie ein Prefferspray - und dann fliehen. Es ist jedoch sinnvoll mehrmals hintereinander zu schießen - auch wechselweise mit Gas- und Knallpartonen, um den Druck auf die jeweils folgende Gaspatrone zu verstärken. Hinzu kommt der laute Knall, er kann zusätzlich irritieren und der Angreifer fürchtet auch - falls er nicht ganz ausgeschaltet ist -, dass Anwohner womöglich die Polizei anrufen usw.

Ist das Magazin leer geschossen und der Angreifer ist immer noch nicht in die Flucht geschlagen kann man mit dem Griff einer Schreckschusswaffe auch zuschlagen.

Eine Schreckschusspistole ist auffälllig und kann schwerer verdeckt getragen werden. Sieht der Angreifer die Pistole, kann es zur Eskalation kommen. Ein weiteres Problem: Auch Unbeteiligte können zunächst nicht unterscheiden ob es sich um eine echte Waffe handelt. Eine echte Gefahrenquelle, auch oder vorallem beim Kontakt mit der Polizei.

Rechtliches
Der Erwerb einer Gaspistole ist erlaubnisfrei. Zum Führen in der Öffentlichkeit wird der „kleine Waffenschein“ benötigt, den man sich bei seiner örlichen Behörde beantragen kann. Dieser Waffenschein muss immer mitgeführt werden. **Hast du kein sauberes Führungszeugnis oder bist bei der Polizei als „Rechts“ eingestuft beantrage lieber niemals einen kleinen Waffenschein und führe dementsprechend auch keine Schreckschusspistole in der Öffentlichkeit, andernfalls kann dir unter umständen sogar ein Mitführverbot von erlaubnisfreien Waffen auferlegt werden!** Abfeuern einer Schreckschusswaffe bei Feiern oder zur Jahreswende

Dieser Beitrag befasst sich mit den räumlichen Rahmenbedingungen in Berlin. Richtig ist

Wer mindestens 18 Jahre alt ist, darf eine zugelassene SRS-Waffe (Schreckschuss-, Reizstoff oder Signalwaffe) kaufen und zu Hause aufbewahren.
Wer einen „Kleinen Waffenschein“ hat, darf eine zugelassene SRS-Waffe in der Öffentlichkeit führen.
Auch wer einen „Kleinen Waffenschein“ hat, darf draußen nicht mit einer SRS-Waffe schießen.
Eine Ausnahme bildet das Schießen mit Platzpatronen auf dem eigenen Grundstück, wozu ausdrücklich nicht der wohnungseigene Balkon zählt.

Was bedeutet das?

Das Schießen mit SRS-Waffen nur zum Vergnügen ist - nicht nur zur Jahreswende - verboten und wird mit empfindlichen Geldbußen geahndet. Wir sind uns sicher, dass du keine Post von den Bullen erhalten möchtest. Lasse also bitte die SRS-Waffen bei Feierlichkeiten oder an Silvester - zu deiner eigenen Sicherheit - am besten Zuhause.

SRS- Schreckschusswaffen Fazit
Schreckschusspistolen sind als Selbstverteidigungsmittel sehr wohl geeignet. Jedoch muss es der Träger einer solchen Waffe auch sein.

10.4 Jet Protector

„Jet Protector“ heißt die Reihe von Pfefferspray-Abwehrsystemen der Schweizer Firma Piexon AG. Die Firma Piexon AG hat die Wirksamkeit von Pfefferspray perfektioniert, denn in der Jet Protector-Reihe werden die Pfefferladungen pyrotechnisch - das heisst mit einer kleinen Treibladung - ähnlich wie bei einer „echten“ Waffe herausgeschleudert.

Der Pfefferstrahl erreicht eine weite von bis zu 6,50 m und weißt einen hohen Druck auf. Die Vorteile liegen auf der Hand:

Die Abwehr von Angreifern in einer hohen Distanz schafft zusätzliche Sicherheit.
Der hohe Druck verstärkt die Wirkung
Die Wirkung wird nicht von Wind- und Wettereinflüssen beeinträchtigt

Es sind zwei verschiedene Modelle erhältlich:

Jet Protector GUARDIAN ANGEL
Das kleine, handliche Gerät passt in die Handtasche oder lässt sich mittels Clip oder Gürteltasche verstauen. Durch einen Auslöser können zwei Pfefferladungen abgegeben werden. Anschließend muss das Gerät ausgetauscht werden. Konzipiert ist das Gerät für die Nahbereichsverteidigung (o,5 - 4 m).

Jet Protector JPX
Dieses Gerät erinnert an die Form einer Pfefferpistole. Gegenüber dem GUARDIAN ANGEL lassen sich die Kartuschen austauschen. Weiteres Zubehör wir Holster, Bauchtaschen sind erhältlich. Für den Alltagsgebrauch ist das Gerät wahrscheinlich etwas groß.

Fazit
Die Geräte der Jet Protector - Reihe sind nicht ganz billig, aber äußerst wirksam. Die ungeschlagende Reichweite schafft zusätzliche Sicherheit.

10.4.1 Kubotan / Tacticalpen

Ein Kubotan ist im Prinzip nichts anderes, als ein kurzer und kleiner Stock welcher ursprünglich als Schlüsselanhänger entwickelt wurde. Erlernt und trainiert wird der Umgang mit einem Kubotan in verschiedenen Kampfsportarten.

Der Kubotan ist im Regelfall einige Zentimeter länger als die Hand des Nutzers. Wird er dann in der Faust gehalten, steht er auf beiden Seiten ein wenig über. Die reguläre Länge von durschnittlichen Kubotan beträgt damit ca. 12-16 cm. Kubotan können quasi aus allen harten Materialien hergestellt werden. Am meisten finden harter Kunststoff, Aluminium und Holz Verwendung. Sie können entweder unauffällig wie ein Stock aussehen oder mit Riffeln zur besseren Griffigkeit ausgestattet sein. Zu den Enden hin laufen Kubotan meist etwas spitz zu, um eine bessere Verteidigungswirkung zu erreichen.

Tacticalpens
Wenn Kubotan die Form eines Kugelschreibers haben - oder zusätzlich sogar Kugelschreiberfunktionen besitzen - spricht man von „Tacticalpens“. Damit kann der Kubotan bequem wie ein herkömmlicher Kugelschreiber überall hin mitgenommen werden und wird im Einsatzfall zur Verteidigungswaffe.

Rechtliche Bewertung
Kubotan bzw. Tacticalpens unterliegen nicht dem deutschen Waffengesetz und können damit frei verkauft und geführt werden (PDF auf der Weltnetzseite des BKA herunterladen oder lade dir die PDF von der s-f-n.org Seite herunter www.s-f-n.org/material).
Kubotan kaufen
Kubotan können in Waffengeschäften oder im einschlägigen Weltnetzhandel erworben werden. Ein Altersnachweis ist nicht notwendig. Es ist keine Erlaubnis (Waffenschein oder Ähnliches) erforderlich.
Bewertung von Tacticalpens bzw. Kubotan
Um mit einem Kubotan sinnvoll und sicher umgehen zu können, ist etwas Training sinnvoll. Auf jeden Fall ist die Verteidigungswirkung eines Kubotan höher, als mit bloßen Fäusten. Da es sich um eine Nahkampfwaffe handelt, ist eine gewisse körperliche Konstitution von Vorteil. Im Ergebnis ist der Kubotan sicher keine Verteidigungswaffe für Jedermann und jeden Fall.

10.4.2 Pfefferspray

Pfefferspray ist als Selbstverteidigungsmittel äußerst beliebt. Nicht nur, dass die Sprays sehr günstig sind, sie sind auch bequem und praktisch überall zu verstauen. Der Wirkstoff aus der Chilipflanze wird mittels Sprühdosen abgegeben und durch einen Pfefferstrahl gegen das Ziel gebracht.

Die Wirkung
Pfefferspray wirkt beim Auftreffen sofort oder innerhalb von wenigen Sekunden. Es wirkt zuverlässig gegen Tiere aller Art (Hunde, Bären usw.) als auch gegen menschliche Angreifer. Nur 2% aller Menschen sind immun gegen Pfefferspray (im Gegensatz zu Tränengas bzw. CS-Gas, hier sind es bis zu 20%). Beim Kauf unbedingt auf die Dosierung achten. Für eine gute und sichere Wirkung sollte diese bei 10
Die Rechtslage
Pfefferspray ist in Deutschland als Tierabwehrspray deklariert. Damit unterliegt es nicht dem Waffengesetz und darf von jedermann erworben und geführt werden (Ausnahme Versammlungen wie Demonstrationen). Der Einsatz ist nur gegen Tiere erlaubt. Im Notwehrfall (Überfall, Angriff, Raub usw.) ist aber auch die Anwendung gegen menschliche Angreifer denkbar.
Pfeffergel, Pfefferschaum
Pfeffergel ist etwas schwerer als Pfefferspray. Dadurch ist der Strahl windstabiler und erreicht eine höhere Reichweite. Pfefferschaum bindet den Wirkstoff am Ziel. Damit werden Unbeteiligte nicht

betroffen. Geeignet in Räumen.
Strahl oder Nebel?
Diese Entscheidung kann dir niemand abnehmen. Entscheide dich je nach gewünschtem Anwendungsgebiet. Der (balistische) Strahl ist etwas windstabiler als der Nebel, außerdem werden höhere Reichweiten ermöglicht. Der (konische) Nebel hat eine größere Wirkfläche, gerade in hektischen, unübersichtlichen Situationen ist es dann wesentlicher einfacher zu treffen.
Anwendung
Ziele auf die Atemorgane des Angreifers bzw. auf die Augen. Nach der Anwendung entfernen dich sofort vom Gefahrenort, da Pfefferspray selten einige Sekunden benötigt bis es wirkt. Verständige die Polizei und Rettungsdienst. Beobachte den Angreifer nach dem Einsatz wenn möglich um der Polizei die Festnahme zu ermöglichen.
Grundsätzliches zur Selbstverteidigung mit Sprays:
Niemals ankündigen, das man Reizgas anwenden wird. Der Gegner wird vorbereitet sein, die Augen schließen und die Luft anhalten, wenn er euch angreift. Das Gas immer überraschend einsetzen, im besten Fall, wenn der Gegner ausgeatmet hat - beobachtet den Brustkorb !

10.5 Schlagstock

Ein Schlagstock ist eine Hiebwaffe aus Metall, Holz oder Gummi. Durch die Verstärkung der Muskelkraft soll ein Angreifer kampfunfähig gemacht werden.

Ein Schlagstock ist als Selbstverteidigungswaffe eher ungeeignet. Die Stöcke sind nicht nur unhandlich und schwierig zu verstauen, sie sind meist auch mehr oder weniger schwer. Für ungeübte Nutzer ist es fast unmöglich, sich nicht entwaffnen zu lassen, jedoch wenn man den Schlagstock unmittelbar nach dem ziehen einsetzt, hat selbst ein Meister nicht die Zeit zu entwaffnen. Das nötige mass an Übung beschränkt sich darauf, den Schlagstock zu ziehen und den ersten Schlag zu machen. **In 99% der Kämpfe ohne Rüstung entscheidet der erste Schlag über den ausgang des Kampfes.**

Weiterhin ist eine schwere Verletzung des Täters wahrscheinlich. Dies könnte anschließend je nach Fall zivilrechtliche Schadensersatzforderungen nach sich ziehen. Im entgegengesetzten Fall ist nach einer Entwaffnung des Opfers durch den Täter eine Verletzung des Opfers wahrscheinlich. Ein Schlagstock kann in Deutschland ab 18 Jahren gekauft werden aber gilt als Waffe (§42a WaffG)! Für das Führen in der Öffentlichkeit muss ein „berechtigtes Interesse“ vorliegen. Dieses Interesse ist (laut dem Bundesinnenministerium) mit dem Argument Selbstschutz nicht gegeben. Hier muss z.B. ein berufliches Interesse (privater Sicherheitsdienst) vorliegen.

Fazit
Ein Schlagstock ist als Mittel zur Selbstverteidigung unpraktisch und eher nicht zu empfehlen. Zu schwer wiegen die Nachteile im Gegensatz zu anderen Mitteln der Selbstverteidigung.

10.6 Schrillalarm

Ein Schrill-Alarm ist ein Alarmgeber, der in einem Notfall Angreifer abschrecken soll. Die kleinen, handlichen Geräte funktionieren dabei ähnlich wie die Fanfaren, die man aus dem Fußballstadion kennt. Im Regelfall wird ein extrem lauter, schriller Ton erzeugt. Dieser liegt meist in der Lautstärke eines startenden Düsenjets.

Dieser Alarmton hat zwei Auswirkungen. Zum einen werden andere Menschen auf eine eventuelle Notsituation aufmerksam. Diese können dann im Fall der Fälle die Polizei verständigen oder gleich selbst zur Hilfe eilen. Zum anderen wird der Angreifer auch physisch abgeschreckt, denn der Alarmton verursacht starke Schmerzen in den Ohren.

Die Vorteile

Einfachst zu handhaben
Keine Nebenwirkungen
Keine Gefahr selbst beeinträchtigt zu werden
Günstig in der Anschaffung
Von der Polizei empfohlen

Die Nachteile

Angreifer wird nicht außer Gefecht gesetzt (wie z.B. bei einem Pfefferspray)
In einer einsamen Umgebung oder bei Nacht ist die Wahrscheinlichkeit von fremder Hilfe gering

Zusammengefasst ist der Schrillalarm eine gute Ergänzung zu anderen Selbstverteidigungswaffen. Ob man sich jedoch alleine auf die kleinen Alarmgeber verlassen sollte, muss jeder selbst entscheiden.

10.7 Selbstverteidigungsschirm

Eine ungewöhnliche Idee - ein Regenschirm zum Selbstschutz? In Amerika ist nichts unmöglich und so wurde auch diese Variante einer Selbstverteidigungswaffe verwirklicht. Aber ist der Schirm zur Selbstverteidigung wirklich sinnvoll und effektiv einzusetzen? Besondere Funktion

Der Schirm unterscheidet sich laut Hersteller hauptsächlich durch seine Stabilität von herkömmlichen Schirmen. Er soll speziell gefertigt und unzerbrechlich sein. Ansonsten hat er die normale Funktion eines Schirmes und schützt dementspechend auch vor Regen.

Als Abwehrwaffe verwendet soll er dann Angriffe wie Tritte, Schläge und Attacken abwehren können. Besonders auch in Kombination mit Sportarten zur Selbstverteidigung soll er gut harmonieren und eine sinnvolle Ergänzung sein.

Äußere Beschaffenheit
Mit 700 Gramm wiegt der Schirm aufgrund seiner Beschaffenheit erwartungsgemäß mehr als ein normaler Regenschirm. Das Aussehen ist als schlicht und elegant zu bewerten. Ein schwarzer, schlanker Regenschirm kann überallhin mitgenommen werden. Die Praxistauglichkeit in Sachen Regenschutz ist also gegeben. Auch keine Aufschrift verrät die besondere Funktion. Zusätzlich hat der Schirm einen automatischen Öffnungsmechanismus.

Rechtliche Bewertung
Auf Flughäfen oder bei Sicherheitskontrollen sind keine Probleme zu erwarten. Der Griff ist aus Polyamid gefertigt, die Spitze aus Metall. Eine Waffenrechtliche Problematik ist nicht erkennbar - es handelt sich einfach nur um einen besonders stabilen Regenschirm. Somit kann der Schirm überall hin mitgenommen werden.

Praxistauglichkeit
Prinzipiell erscheint der Schirm zunächst einmal eine gute Sache zu sein. Allerdings bleibt die Frage, ob der Schirm nicht eher für Regentage mit sich geführt wird - niemand wird den Schirm im Hochsommer bei 30 Grad ständig mit sich führen wollen. Weiterhin ist der Schirm vermutlich nicht für jedermann geeignet. Eine gewisse Sicherheit im Umgang mit Schlagwerkzeugen erscheint sinnvoll.

10.8 Taktische Taschenlampe

In der langen Dunkelheit des Winters kannst du dich mit einfachen Mitteln effizient schützen. Nutze die Vorteile der Dunkelheit durch die taktische Nutzung einer Taschenlampe.

Hierbei handelt es sich um eine kleine Taschenlampe die äußerst robust gerfertigt wird und ebenfalls wie ein Kubotan benutzt werden kann. Außerdem ist sie natürlich ideal für dunkle Keller, Parkhäuser und sonstige Orte mit schlechten Lichtverhältnissen.

Inzwischen nutzen diese Lampen günstige Batterien (AA oder AAA) und nicht mehr die teuren Fotobatterien. Die Blendwirkung ist selbst bei vorhandenem schwachen Licht noch immer gut und ermöglicht so einen weiteren taktischen Einsatz. Einige Versionen dieser Lampen verfügen über einen Stroboskop-Effekt um einen möglichen Angreifer noch mehr zu stören

Problem Batterie
Die Batterien in der Taschenlampe können sich entladen, wenn sie nicht regelmäßig überprüft werden. Dann ist das Gerät im Einsatzfall wirkungslos.
Fazit
Zum Zwecke der Selbstverteidigung sind taktische Taschenlampen durchaus zu empfehlen. Natürlich empfiehlt sich auch hier eine gewisse Übung mit der Lampe aber immerhin fallen sie nicht unter das Waffengesetz (WaffG) und können somit auch auf Veranstaltungen problemlos geführt werden.

11 Rechtsratgeber

Das Buch **„Mäxchen Treuherz und die juristischen Fußangeln"** wurde im Jahre 1990 geschrieben, um der bei politischen Aktivisten herrschenden Unwissenheit und Unsicherheit in juristischen Fragen entgegenzutreten. Damals, als die Teilung Deutschlands endete, glaubten viele, besonders in den neuen Bundesländern, dass hierzulande nun die absolute Freiheit herrsche und jeder politisch reden und handeln könne, wie er wolle.

Doch die Grundrechte gelten nicht absolut, sondern sind beschränkt durch die Rechte anderer gemäß des richtigen Grundsatzes „Meine Freiheit endet da, wo Deine Freiheit beginnt", - wobei man sich trefflich darüber streiten kann, ob man die von unseren Gerichten gezogenen Grenzen in jedem Falle bejahen kann oder sie nicht vielmehr kritisieren muss. Diese Grenzen sind aber geltendes Recht und wer sie missachtet, der muss sich auf Strafen, Verbote und hohe finanzielle Verluste einstellen.

Da es sinnvoller erscheint, Kräfte, Energien und Gelder für die politische Auseinandersetzung im Volke, aber nicht für Geldstrafen, Geldbußen und Gerichtskosten auszugeben, wurde „Mäxchen Treuherz" verfasst, vielfach überarbeitet und jetzt neu herausgegeben, damit

die bereits bestehenden Grenzen zwischen Erlaubtem und Verbotenem beachtet werden können rechtswidrige Maßnahmen der Behörden oder politischer Gegner mit juristischen Mitteln erfolgreich bekämpft werden können und die Rechtsprechung sich hinsichtlich der Grenzen der Freiheitsrechte weiterentwickeln und verbessern kann.

Als Ergänzung zu dem Buch „Mäxchen Treuherz und die juristischen Fußangeln" ist jetzt auch eine Multi-Media-Doppel-CD hierüber erschienen. Die CD ist in 8 Kapitel unterteilt die du dir bei uns anhören kannst. Die Geschichten werden vorgelesen, um einen Einstieg in die auftretenden juristischen Schwierigkeiten zu ermöglichen.

11.1 Rechte im Umgang mit der Polizei in Brandenburg

Oft kommt es vor, dass Polizeibeamte fast schon willkürlich gegen Widerstandskämp-

fer vorgehen, ohne sich an gesetzliche Vorgaben zu halten. Dies ist zu großen Teil der Repressivmanier des Systems, leider aber auch der Unkenntnis vieler Widerstandskämpfer zu danken, wenn es um die Rechte und Pflichten vollziehender Polizeibeamter geht. Der folgende kommentierte Auszug aus dem Brandenburgischen Polizeigesetz (BbgPolG) soll dazu beitragen, die eigenen Rechte gezielt wahrzunehmen und damit gegen Willkürakte auf dem Verwaltungsrechtsweg vorgehen zu können. Auch die Kenntnis der eigenen Rechte schützt dich nur dann, wenn du bereit bist, sie auch durchzusetzen

11.1.1

Im Umgang mit Polizisten steht man allzu oft einer anonymen Staatsmacht gegenüber, derer man sich schon deshalb nicht erwehren kann, weil man keinen der vollziehenden Beamten namentlich kennt. Eine spätere „Beschwerde“ erscheint also unmöglich. Dies würde - sofern es denn rechtens wäre - den grundgesetzlich verbrieften Rechtsstaat aushebeln. Daher heißt es in

Paragraph 9 Legitimationspflicht

Auf Verlangen des von einer Maßnahme Betroffenen hat sich der Polizeivollzugsbedienstete auszuweisen, soweit der Zweck der Maßnahme dadurch nicht beeinträchtigt wird.

Dies bedeutet für dich: Der Polizist, der dich durchsucht, befragt, oder einfach „nur“ deine Personalien aufnehmen will, muss auf Nachfrage seinen Namen, seine Dienstnummer und seine Dienststelle angeben. Im Einzelfall wird der Polizist sich auf Anordnungen seines Einsatzleiters berufen. Damit will er sein eigenes Vorgehen rechtfertigen. In diesem Fall erfrage auch den Namen und die Dienststelle des Einsatzleiters. Dem Zweck der Maßnahme steht dies praktisch nur entgegen, wenn vermummte SEK - Beamte oder polizeiliche V - Leute agieren (Diese wird man aber ohnehin selten nach ihrem Ausweis fragen wollen). Auf diesen Ausschlussgrund kann sich damit in der Praxis so gut wie kein Polizist berufen. **Schreibe dir auf, was der Polizist zu seiner Legitimation vorträgt - alles Andere ist schnell vergessen!**

Für die Durchsetzung deiner nachfolgend beschriebenen Rechte ist die Kenntnis des verantwortlichen Beamten stets Voraussetzung - das weiß auch jeder Polizist und daher sind unangenehme Situationen oft schon im Vorfeld vermeidbar, wenn der Beamte persönliche Konsequenzen für unsachgerechtes Handeln befürchten muss. Bringe daher bei jeder staatlichen Maßnahme so früh wie möglich in Erfahrung, mit wem du es zu tun hast!

11.1.2 Befragung - was musst Du sagen ?

Beachte bitte das Kapitel: Aussageverweigerung

Bei Befragungen der Polizei gilt grundsätzlich alles, was für Beschuldigte und Zeugen im Strafverfahren gilt (Aussageverweigerungsrecht des Beschuldigten, Zeugnisverweigerungsrecht für Angehörige und Zeugen, die sich selbst belasten müssten). Eine Belehrung hierüber bleibt in der Praxis oft aus. Dies ist zwar ein Verfahrensfehler, kann aber schlecht bewiesen werden und führt nicht zur Nichtigkeit evtl. gemachter Aussagen.

§ 11 Befragung, Auskunftspflicht

Absatz 1: Die Polizei kann jede Person befragen, wenn Tatsachen die Annahme rechtfertigen, dass sie sachdienliche Angaben machen kann, die für die Erfüllung einer bestimmten polizeilichen Aufgabe erforderlich sind. Für die Dauer der Befragung kann die Person angehalten werden.
Absatz 2: Eine Person, deren Befragung nach Absatz 1 zulässig ist, ist verpflichtet, auf Frage Namen, Vornamen, Tag und Ort der Geburt, Wohnanschrift und Staatsangehörigkeit anzugeben. (...)

Absatz 3: Zur vorbeugenden Bekämpfung der grenzüberschreitenden Kriminalität kann die Polizei im öffentlichen Verkehrsraum angetroffene Personen kurzzeitig anhalten, befragen und verlangen, dass mitgeführte Sachen in Augenschein genommen werden. Die Maßnahme ist nur zulässig, wenn aufgrund von Lageerkenntnissen anzunehmen ist, dass Straftaten von erheblicher Bedeutung (§ 10 Abs. 3) begangen werden sollen. Ort, Zeit und Umfang der Maßnahme dürfen nur durch den Polizeipräsidenten oder seiner Vertreter im Amt angeordnet werden.

Du siehst: Bis auf deine Personalien musst du den Polizisten gegenüber grundsätzlich keine Angaben machen. Absatz 3 bezieht sich auf Zollgrenzbezirke. In diesen Bereichen (z.B. Grenzbereich zu Polen) benötigt die Polizei keinen richterlichen Durchsuchungsbeschluss, wenn z.B. Fahrzeuge durchsucht werden sollen. Informiere dich also rechtzeitig ob dich deine Fahrt in solche Gegenden führt - treffe nötigenfalls Vorkehrungen. „Straftaten von erheblicher Bedeutung“ sind alle Verbrechen (d.h. Straftaten, die mit mindestens einem Jahr Freiheitsstrafe bedroht sind) und alle in Paragraph 100a StPO aufgeführten Delikte (hierzu Zählen z.B. auch §§ 86, 129, 130 etc.)

11.1.3 Durchsuchung von Personen und Sachen

Personen
Oftmals wollen Beamte einen Blick in deinen Kofferraum oder in deine Hosentaschen werfen. Betrachten wir zunächst die Durchsuchung von Personen:

§ 21 Durchsuchung von Personen

Absatz 1: Die Polizei kann außer in den Fällen des § 12 Abs. 2 Satz 4 eine Person durchsuchen, wenn

sie nach diesem Gesetz oder anderen Rechtsvorschriften festgehalten werden kann,
Tatsachen die Annahme rechtfertigen, dass sie Sachen mit sich führt, die
sichergestellt werden dürfen,
sie sich erkennbar in einem die freie Willensbestimmung ausschließenden Zustand oder sonst in hilfloser Lage befindet,
sie sich an einem der in § 12 Abs. 1 Nr. 2 genannten Orte aufhält oder
sie sich in einem Objekt im Sinne des § 12 Abs. 1 Nr. 3 oder in dessen unmittelbarer Nähe aufhält und Tatsachen die Annahme rechtfertigen, dass in oder an Objekten dieser Art Straftaten begangen werden sollen, durch die Person oder diese Objekte gefährdet sind.
Absatz 2: Die Polizei kann eine Person, deren Identität nach diesem Gesetz oder anderen Rechtsvorschriften festgestellt werden soll, nach Waffen, anderen gefährlichen Werkzeugen und Explosivmitteln durchsuchen, wenn das nach den Umständen zum Schutz des Polizeivollzugsbediensteten oder eines Dritten gegen eine Gefahr für Leib oder Leben erforderlich erscheint. Dasselbe gilt, wenn eine Person nach anderen Rechtsvorschriften vorgeführt oder zur Durchführung einer Maßnahme an einen anderen Ort gebracht werden soll.
Absatz 3: Personen dürfen nur von Personen gleichen Geschlechtes oder Ärzten durchsucht werden; das gilt nicht, wenn die sofortige Durchsuchung zum Schutz gegen eine Gefahr für Leib oder Leben erforderlich ist.

Auffällig ist hier, dass die Polizei einen sehr weiten Spielraum genießt, wenn es um die Personendurchsuchung geht: Zwar darf sie „nur“ bestimmte Sachen suchen (Waffen, Sprengstoff etc.) - und das nur, wenn „Gefahren für Leib und Leben“ drohen, doch selbstverständlich dürfen Zufallsfunde (Flugblätter, verfassungsfeindliche Symbole etc.) dennoch verwendet werden. Diese Vorschrift kann in der Praxis sehr gefährlich werden, räumt sie den Beamten doch große Freiheiten ein. Beachte deshalb, keine überflüssigen Gegenstände mitzuführen, die bei Durchsuchungen eine Anzeige rechtfertigen würden!
Um übermäßiger Repression zu begegnen, beachte die Hinweise zur Ausweispflicht der Polizisten und gehe gegen jede Personendurchsuchung auf dem Rechtsweg vor, sofern sie erfolglos und offensichtlich unverhältnismäßig war.

Sachen
Um gegen Durchsuchungen vorgehen zu können, ist es wichtig, beweisen zu können, dass sie überhaupt stattgefunden haben. Dazu gilt

§ 22 Durchsuchungen von Sachen

Absatz 1: Die Polizei kann (...) eine Sache durchsuchen, wenn
sie von einer Person mitgeführt wird, die nach § 21 durchsucht werden darf,
Tatsachen die Annahme rechtfertigen, dass sich in ihr eine Person befindet, die
in Gewahrsam genommen werden darf,
widerrechtlich festgehalten wird oder
hilflos ist,
Tatsachen die Annahme rechtfertigen, dass sich in ihr eine andere Sache befindet, die sichergestellt werden darf, sie sich in einem der in § 12 Abs. 1 Nr. 2 genannten Orte befindet,
sie sich in einem Objekt im Sinne des § 12 Abs. 1 Nr. 3 oder in dessen unmittelbarer Nähe befindet und Tatsachen die Annahme
rechtfertigen, dass in oder an Objekten dieser Art Straftaten begangen werden sollen, durch die Personen oder diese Objekte gefährdet sind, oder
es sich um ein Land-, Wasser- oder Luftfahrzeug handelt, in dem sich eine Person befindet, deren Identität nach § 12 Abs. 1 Nr. 4 oder 5 festgestellt werden darf; die Durchsuchung kann sich auch auf die in dem Fahrzeug enthaltenen Sachen erstrecken.
Absatz 2: Bei der Durchsuchung von Sachen hat der Inhaber der tatsächlichen Gewalt das Recht, anwesend zu sein. Ist er abwesend, so sollen sein Vertreter oder ein anderer Zeuge hinzugezogen werden. Dem Inhaber der tatsächlichen Gewalt ist auf Verlangen eine Bescheinigung über die Durchsuchung und ihren Grund zu erteilen.

„Inhaber der tatsächlichen Gewalt“ bist du auch, wenn du ein Auto deines Freundes fährst, eine Tasche deiner Schwester dabei hast etc. - Du kannst also gemäß § 22 Abs. 2 Satz 3 BbgPolG eine Bescheinigung über die Durchsuchung und ihren Grund verlangen. Von diesem Recht solltest du unbedingt Gebrauch machen, und zwar deshalb:

„Gefahr im Verzug“?
Sehr gern berufen sich Polizeibeamte auf das Vorliegen von „Gefahr im Verzug“. Damit ist gemeint, dass der Zweck der Durchsuchung gefährdet würde, wenn erst ein Durchsuchungsbeschluss des zuständigen Amtsrichters eingeholt werden müsste. Dies gilt eigentlich für Fälle wie diesen:

Ein Räuber ist nachts auf der Flucht und hat die Beute im Kofferraum, die Polizei verfolgt ihn seit der Tat. Nun hält sie ihn an und möchte in den Kofferraum schauen. Mitten in der Nacht wird es keinen Durchsuchungsbeschluss mehr geben, da der Richter längst schläft. Im Verzug der Durchsuchung liegt aber die Gefahr für den Ermittlungserfolg. Daher dürfen die Beamten jetzt auch ohne Beschluss durchsuchen.

Anderes gilt offenbar für Widerstandskämpfer:

Sonntag, 8 Uhr.
Eine gut geplante Durchsuchung findet zeitgleich in mehreren Objekten und durch 40 Beamte statt - auch hier ohne Durchsuchungsbeschluss, „Gefahr im Verzug“.

Hat man am Freitag keinen Amtsrichter mehr gefunden, oder lag einfach kein Grund vor, weshalb kein Richter den Beschluss unterschrieben hätte? Egal - für dich heißt das: Du brauchst unbedingt eine Bescheinigung über die Durchsuchung.

Wenn etwas gefunden wird, bekommst du ein Protokoll. Nach § 22 Abs. 2 Satz 3 BbgPolG muss

hierauf auch ein Grund der Durchsuchung angegeben werden, wenn du dies verlangst. Bundesdeutsche Gerichte haben schon entschieden, dass Durchsuchungen rechtswidrig und beschlagnahmte Gegenstände herauszugeben sind, wenn sich herausstellt, dass keine Gefahr im Verzuge vorgelegen hat. Dies sollte man auf jeden Fall beachten, denn unter diesen Umständen können Zufallsfunde auch hierzulange einem (z.B. in den USA üblichen) Beweisverwertungsverbot unterliegen. Ein weiterer Grund, weshalb man auch bei erfolgloser Durchsuchung auf die Aushändigung der Bescheinigung bestehen sollte: Die Polizeistatistik rühmt sich mit „Spürsinn". Bei Gefahr im Verzug wird immer etwas gefunden - aber nur, weil bei erfolglosen Durchsuchungen kein Protokoll ausgefüllt wird, der Beamte keinen Bericht schreibt und die Durchsuchung dann theoretisch gar nicht stattgefunden hat! Um diesem Missstand entgegenzuwirken, sollte immer die Bescheinigung gefordert und auch gegen erfolglose Durchsuchungen vorgegangen werden - schließlich greifen auch (und gerade) diese in dein grundgesetzlich verbürgtes Persönlichkeitsrecht ein!

11.1.4 Verhältnismäßigkeit

Bei allen Maßnahmen des Staates gegen seine Bürger steht der Grundsatz der Verhältnismäßigkeit im Vordergrund. So auch im Polizeirecht:

§ 3 Grundgesetz der Verhältnismäßigkeit

Absatz 1: Von mehreren Möglichkeiten und geeigneten Maßnahmen hat die Polizei diejenige zu treffen, die den Einzelnen und die
Allgemeinheit voraussichtlich am wenigsten beeinträchtigt.
Absatz 2: Eine Maßnahme darf nicht zu einem Nachteil führen, der zu dem erstrebten Erfolg erkennbar außer Verhältnis steht.
Absatz 3: Eine Maßnahme ist nur solange zulässig, bis ihr Zweck erreicht ist oder sich zeigt, dass er nicht erreicht werden kann.

Dies liest sich zunächst wie eine Garantie für einwandfreies rechtsstaatliches Handeln. Doch leider lässt sich kaum ein Einsatzleiter gern auf die Unverhältnismäßigkeit seiner Maßnahme hinweisen, vor allem nicht, wenn sowieso niemand seinen Namen kennt. Nach dem sorgfältigen Studium dieser Seiten solltest du aber hier bereits den Namen des Einsatzleiters kennen. Jetzt weißt du auch, dass er an den Grundsatz der Verhältnismäßigkeit gebunden ist und dass du - falls er das vergessen sollte - vor den Verwaltungsrichtern dagegen vorgehen wirst. Natürlich sind auch Gerichte keine Waffenbrüder für nationale Freiheitskämpfer und oft entscheiden sie zugunsten der Polizei. Weise deshalb den Einsatzleiter / Polizisten sachlich, freundlich (er ist auch nur ein Werkzeug des Systems, kein „schlechter Mensch") aber bestimmt darauf hin, dass du deine Rechte kennst und dass du weißt, wie du sie auch nachträglich einklagen kannst. Wenn du alles hier Geschriebene beherzigst, benötigst du dazu noch nicht mal einen Anwalt, nur etwas Zeit und ein Gedächtnisprotokoll der Vorgänge, mit denen du nicht einverstanden bist.

11.1.5 Nachwort

Ähnliche Polizeigesetze gibt es in jedem Bundesland, sie unterscheiden sich meist nur in den Nummern der Paragraphen. Daher ist dieser Artikel nicht nur in Brandenburg hilfreich - ein Blick ins Polizeigesetz des „Zielgebietes" kann helfen, auch hier die passenden §§ im Gespräch mit der Staatsmacht parat zu haben. **Wer seine Rechte nicht wahrnimmt, muss sich nicht über den „Polizeistaat" beschweren - er begünstigt diesen geradezu durch den freiwilligen Verzicht auf seine Rechte**

11.2 Verfassungsschutz - Anquatschversuche

Während der Staatschutz in der Regel darauf aus ist, konkrete Informationen über Zusammensetzung und Aktionen unserer Zusammenhänge zu kriegen, um aus ihnen Konstrukte bilden zu

können, die sie gegen uns verwenden wollen, verfolgt der Verfassungsschutz vornehmlich das Ziel, einen detaillierten Gesamtüberblick über den Widerstand zu bekommen. Er soll durch seine Analysen und Prognosen dazu beitragen, die geeignetsten Mittel des Repressionsapparates zur Sicherung seiner Herrschaft herauszufinden. Auf der Grundlage der Erkenntnisse des VS entscheiden die Strategen der „inneren Sicherheit“, wie versucht werden soll den Widerstand zu brechen.

Der Verfassungsschutz ist dabei ständig bemüht, unsere politische Arbeit zu bewerten und vorauszusehen, inwieweit sie die herrschende Ordnung gefährden könnte. Dafür erhält es der Verfassungsschutz für notwendig, alle möglichen Interna, Diskussionen und Funktionen von Leuten aufzuzeichnen und nachvollziehen zu können. Dabei gibt es einen regen Informationsaustausch zwischen Politbullen und VS und über das gesetzlich erlaubte hinaus auch eine informelle Koordination und enge Zusammenarbeit wenn es um ein gemeinsames Ziel geht, bspw. die Kriminalisierung eines bestimmten Zusammenhanges oder Projektes.

Der Verfassungsschutz bedient sich verschiedener Arbeitsweisen, beispielsweise dem Auswerten von öffentlich zugänglichen Quellen wie Netzseiten, Broschüren, Zeitschriften und Veranstaltungen, Informationsbeschaffung bei (dazu verpflichteten) staatlichen Institutionen wie Uni, Schule, Amt usw. aber auch Anfragen bei Arbeitgeber, Familie, Freunden und Bekannten, dem Einsatz von Spitzeln und den Anwerbeversuchen.

Der Verfassungsschutz versucht kontinuierlich Informanten durch das Anwerben von Leuten aus unseren Zusammenhängen zu gewinnen. Er sucht sich die Leute, der er ansprechen will, genau aus und bringt im Vorwege einiges über sie in Erfahrung. So kann er die Umstände und die Taktik des Anwerbeversuches genau auf die Person anpassen, Ort und Zeit bestimmen und den Verlauf vorausplanen. Der Überraschungseffekt im Moment der Kontaktaufnahme ist für dich um so größer. Meist wirst du in einer scheinbar x-beliebigen Situation auf der Straße angesprochen, aber auch Hausbesuche und seltener Telefonanrufe oder Briefe gehören zu ihrem Programm. Die Gesprächsstrategie ähnelt dabei der Verhörtaktik der Bullen.

Zum einen versuchen sie dich verschiedenartig unter Druck zu setzen. Sie nennen beispielsweise anstehende Verfahren, interne Erkenntnisse über dich und deine Umgebung oder andere Umstände, von denen sie meinen, dass sich dich erpressbar machen. Dabei können sie drohend, scheinbar bestechlich oder handgreiflich werden. Zum anderen sind sie darauf aus das Gespräch durch vermeintlich belanglose Themen und einfache, plumpe oder lächerliche Fragen aufrechtzuerhalten. Sie reden über Hobbys, Arbeit und Privates, vermeiden Reizwörter, benutzen Szenevokabular. Dabei versuchen sie immer wieder auf die für sie interessanten Bereiche zu lenken, stellen hier weniger Fragen, sondern treffen Feststellungen, wollen mit dir ein gegenseitiges „Zweckbündnis“ eingehen und stellen andauernd rhetorische Fallen. Je länger dieses Gespräch dauert desto mehr Informationen kriegen sie aus dir heraus. Sie sind geschult und können aus eigentlich bedenkenslosen Äußerungen oder plötzlichen Schweigen, minimalen körperlichen Reaktionen, Mimik und Gestik bereits Erkenntnisse gewinnen, die sie auch verwerten können.

Deine Konsequenz sollte deshalb nur eine sein: Maul halten und den Kontakt sofort abbrechen. Es ist ein grundsätzlicher Fehler sich auf Gespräche mit dem Agenten einzulassen. Es wird kaum möglich sein, irgend etwas Interessantes aus diesen Leuten herauszubekommen und wenn, nur unter Preisgabe viel gewichtigerer Sachen für sie. Du solltest diese Anquatschversuche genauso bewerten wie Angriffe von Bullen und Justiz. Durch ihre Arbeit als Teil des Repressionsapparates beteiligen sie sich an der Kriminalisierung und Zerschlagung des Widerstandes. Zumal die Anquatschversuche aktiv dabei mitwirken sollen, Leute zu lähmen, einzuschüchtern und mit Repression zu bedrohen. Das einzig richtige Verhalten diesen geheimdienstlichen Tätigkeiten entgegenzutreten, ist die Öffentlichkeit zu suchen. Rede mit vertrauten Leuten darüber, fertige ein Gedächtnisprotokoll an und Informiere eine Gruppe zur Veröffentlichung.

Für Anwerbeversuche gilt:

Verweigere dich den Anquatschversuchen der Systemwächter. Sage deutlich, dass du zu keinem Gesprächen mit ihnen bereit bist. Es besteht überhaupt keine Pflicht mit Bullen oder Agenten zu sprechen. Es ist zum Schutz des Widerstandes und zur eigenen Sicherheit wichtig, dass solche Anquatschversuche bereits am Anfang konsequent abgeblockt werden

Fotografiere den Systemwächter mit der Kamera deines Mobiltelefons. Das sollte ihn abschrecken und die Bilder können andere schützen

Findet der Anquatschversuch in der Öffentlichkeit statt, schrei laut heraus, dass es sich um einen Agenten des Systems handelt. Laß die Menschen um dich herum wissen, dass die Überwachung und Unterdrückung unseres Volkes noch genau so real ist, wie vor dem Fall der Mauer

Informiere deine Freunde über den Anquatschversuch, fertige ein Gedankenprotokoll an und sende es zur Veröffentlichung an eine Netzseite in Deiner Region

Lade die Jingles der AG Anquatschversuche herunter. Versende sie an Freunde, brenne sie auf CDs oder spiele sie bei Feiern ab. Schütze dich und deine Kameraden gegen die Angriffe der

11.2.1 Von wem wirst Du angequasselt?

In der BRD gibt es verschiedene staatliche Stellen, die systemkritische oppositionelle Bewegungen und Menschen beobachten, einschüchtern, infiltrieren und zersetzen sollen. Der Inlandsgeheimdienst „Verfassungsschutz“ ist dabei federführend, aber auch die politische Polizei - vertreten durch Landeskriminalämter (LKA) und Bundeskriminalamt (BKA) - versucht Spitzel anzuwerben bzw. schleust Beamte Undercover als Spitzel in systemkritische Bewegungen ein.

Eine Besonderheit im Überwachungsapparat stellt der MAD (Militärischer Abschirmdienst) dar, der vorrangig Bundeswehrsoldaten in die Zange nimmt, wenn sie als politische Aktivisten auffällig geworden sind.

Zum „Auffällig werden“ genügt übrigens schon eine simple Polizeikontrolle im Vorfeld einer Demonstration, einer Saalversammlung, eines Konzertes etc., wo du deine Personalien angeben musstest.

Die genannten staatlichen Stellen haben einen klaren Auftrag: Sie sollen jegliche politische Opposition, die sich kritisch gegen das System stellt, mit allen Mitteln unschädlich machen.

In der BRD gibt es de facto nur noch eine politische Opposition, die dem System unangenehm ist und deshalb bekämpft wird: **Die nationale Opposition.**

Der nationale Widerstand, als junge aktive Basis und Speerspitze der nationalen Opposition, befindet sich dabei besonders im Fadenkreuz der politischen Verfolgungsbehörden, denn dieser Widerstand ist im Laufe der Jahre trotz aller Verfolgung immer größer geworden und kann durch öffentliche Protestaktivitäten die Zustände in der BRD auch für Millionen ahnungsloser Volksgenossen immer weiter sichtbar machen. Das will das System um jeden Preis unterbinden. Du wirst also angequasselt von Mitarbeitern der Verfolgungsbehörden. Sie kommen entweder zu zweit oder auch alleine auf dich zu und wollen dich mit einem Gespräch für eine Spitzeltätigkeit anwerben.

Diese Typen werden im Fachjargon „V-Mann-Führer“ genannt, weil sie „ihren“ Spitzel von Anfang bis Ende betreuen. Man kann sie mit Zuhältern vergleichen, die „ihre“ Prostituierten „laufen lassen“, um für Geld eine niedere Schmutzarbeit zu verrichten.

11.2.2 Warum wirst gerade DU angequasselt?

Der „Verfassungsschutz“ (im folgenden auch „VS“ genannt) und politische Polizei brauchen für ihren Auftrag vor allem eines: Einen fortwährenden Informationsfluss über alles, was sich an der aktiven Basis der nationalen Opposition abspielt.

Einen großen Teil der benötigten Informationen können sie dank der Fahrlässigkeit und Geschwätzigkeit innerhalb der „Szene“ sehr leicht durch Post- und Telefonüberwachung (was bekanntlich den eBrief und Weltnetzverkehr einschließt) aus der aktiven Basis heraussaugen. Doch viele Informationen werden für die Verfolgungsbehörden erst wertvoll, wenn sie durch persönliche Erfahrungen und Einschätzungen sowie aktuelle interne Erkenntnisse ergänzt und in den richtigen Zusammenhang gebracht werden.

Deshalb sind Spitzel (angeworbene Personen; verharmlosend auch „Informanten“ genannt) und Undercoveragenten (eingeschleuste Staatsbeamte) für sie unerlässlich.

Eingeschleuste Staatsbeamte sind im Verhältnis zu Spitzeln eher eine kleine Minderheit, weil sie gerade in freien Zusammenhängen und kleinen Kameradschaften schwer zu etablieren sind. Das System bevorzugt lieber Personen, die sich bereits im nationalen Widerstand befinden, denn die sind zunächst über jeden Verdacht erhaben. Sie sind irgendwann freiwillig und meist auch aus ehrlicher Absicht zur aktiven Basis gekommen und sind in einem gewissen Umfeld etabliert. Darum ist es aus unserer Sicht auch besonders verwerflich, wenn gerade eine solche Person heimlich die Fronten wechselt und plötzlich mit dem Feind kooperiert, der unsere Freiheitsbewegung zersetzen will. Glaube nicht, dass nur langgediente Aktivisten angequasselt werden. Für die Verfolgungsbehörden sind auch scheinbar unwichtige, unbekannte Aktivisten von Bedeutung, wenn sie glauben, dass derjenige eine gute Quelle sein könnte oder sich anderweitig ausnutzen lässt.

Glaube also nicht, dass du zufällig angequasselt wirst. Wenn VS und politische Polizei dich als Spitzel anwerben wollen, dann haben sie sich vorher schon eingehend mit dir befasst. Sie wissen, in welchem Umfeld du dich aufhältst und welche Bedeutung du innerhalb dieses Umfeldes hast. Sie wissen, welche politischen Aktivitäten du betreibst, sie kennen dein privates Umfeld, deine Lebensverhältnisse. Wenn sie dich dann ansprechen, haben sie bereits eine recht genaue Vorstellung davon, welche Informationen sie von dir kriegen und für welche Spitzelaufgaben sie dich einsetzen könnten. Vielleicht wollen sie interne Informationen aus deiner Gruppe absaugen, vielleicht wollen sie dich aber auch zu Straftaten anstiften, mit denen du dein Umfeld kriminalisieren sollst.

Kriminalisierung hat Repression zur Folge: Hausdurchsuchungen, Gerichtsverfahren, Verbote. Aktivisten kommen in Haft, verlieren ihre Arbeit, ihre Wohnung. Der Bewegungsfreiraum aktiver Gruppen wird empfindlich eingeschränkt, die politische Aufbauarbeit kann um Jahre zurückgeworfen werden. Und alles nur, weil DU für eine Handvoll Euros schwach geworden bist...

11.2.3 Was tun, wenn du angequasselt wirst?

Kein ehrlicher Aktivist wird freiwillig zum Verräter, aber einige werden es doch, weil sie das Ganze auf die leichte Schulter nehmen und dann im entscheidenden Moment schwach werden. Du musst dir also schon vorher überlegen, wie du mit der Situation des „Angequasselt Werdens“ umgehen musst. Wie bereits geschildert, wird niemand einfach nur zufällig angequasselt. VS und politische Polizei suchen sich ihre „Kandidaten“ gründlich aus und überlegen sich genau, wie sie dich ansprechen. Jeder hat seine charakterlichen Stärken und Schwächen, jeder ist für dieses oder jenes empfänglich. Beim ersten Kontakt zählt für die nur eines: Sie wollen auf jeden Fall mit dir ins Gespräch kommen!

Haben sie das geschafft, dann wird es für dich schwer, da wieder raus zukommen. Diese Typen sind psychologisch geschult und haben Erfahrung im Anquasseln. Sie tun das jeden Tag - für dich

dagegen ist die ganze Situation völlig neu. Der Überraschungsmoment ist einfach zu groß, als dass du sofort klare Gedanken fassen könntest. Du glaubst, du hättest vielleicht nur ein paar belanglose Sätze gesagt, womit die doch gar nichts anfangen können. Irrtum! Schon die Tatsache, dass du überhaupt bereit bist, dich mit diesen Typen zu unterhalten, offenbart deine persönliche Schwäche.

Darum: Lass es einfach!

Es kann ohnehin nichts geben, was du mit diesen Typen zu bequatschen hättest. Sie sollen dich gefälligst in Ruhe lassen und das musst du ihnen auch sofort sagen, noch ehe sie dich in ein Gespräch verwickeln können. Es sind gar nicht so sehr die Worte, mit denen du ungewollt dein Innerstes offenbarst, sondern vielmehr deine ganze Gestik, deine äußere Haltung dabei. Sie beobachten dein Verhalten und können anhand dessen schon abschätzen, ob du Schwächen hast, die sie ausnutzen können. Zum Überraschungsmoment gehört auch, dass das erste Anquasseln an einem Ort und zu einem Zeitpunkt geschieht, wo du selbst am wenigsten damit rechnest. Sie suchen dich an deinem Arbeitsplatz oder Arbeitsweg auf, vor deiner Schule, vor deiner Firma.

Sie wollen dir das Gefühl geben, dass sie furchtbar viel über dich wissen - sogar wo du arbeitest, zur Schule gehst oder in welchem Sportverein du an bestimmten Wochentagen trainierst. Das ist reine Einschüchterungstaktik! Am besten, du zeigst dich überhaupt nicht überrascht, wenn es soweit ist. Zeig am besten gar keine Reaktion, wenn sie dich anquasseln, sondern bleib äußerlich ganz gelassen.

Sei dir über eines bewusst:
Diese Typen, die dich im Auftrag des Systems anwerben wollen, sind ganz niederträchtige und ehrlose Subjekte. Lästige Schmeißfliegen, die ihr kleines Dasein damit fristen, anderen Menschen hinterher zu schnüffeln und sie auszusaugen. Vor diesen Handlangern brauchst du weder Respekt noch Angst haben. Es hat für dich keinerlei Folgen, wenn du ihnen klipp und klar sagst, dass sie dich nicht belästigen sollen.

Oft kommt es bei solchen ersten Anwerbeversuchen vor, dass die Typen zu dir sagen, dass du ja gar nicht mit ihnen sprechen bräuchtest, sondern einfach erst mal nur zuhören sollst. Das klingt gut, denkst du, denn beim Zuhören passiert ja nichts.

Wirklich nicht? - Erfahrungsgemäß läuft der dann folgende Monolog ungefähr so ab:

Sie erzählen dir einige Dinge über dich und dein politisches Umfeld. Scheinbar zufällig fließen da auch Dinge mit ein, wo du bestimmt gedacht hast, dass die das gar nicht wissen können. Das verunsichert dich. Und das soll es auch. Während sie erzählen, beobachten sie deine Reaktionen und Regungen. Deine Augen, dein Gesichtsausdruck, deine Haltung - das alleine verrät schon an der einen oder anderen Stelle, ob der Monolog Wirkung zeigt oder nicht. Meist dauert es dann nicht lange, bis der Betroffene das Gefühl hat, er müsse jetzt mal was dazu sagen, etwas richtig stellen oder gar abstreiten. Das Gespräch beginnt - ihr Ziel ist erreicht.

Sei dir über eines bewusst:
Alles was sie „wissen“, ist nur antrainiertes Wissen.
Lass dich davon nicht beeindrucken.
Besser noch: Höre es dir erst gar nicht an!

Schon zu viele Betroffene haben sich in ein Gespräch verwickeln lassen, weil sie „nur“ zugehört haben. Und sie haben noch geglaubt, sie würden etwas Nützliches „heraushören“ können. Das ist gefährlicher Unfug! **Diese psychologisch geschulten, routinierten Typen lassen sich nicht in die Karten sehen.**

Die Behauptung, man hätte sich auf Gespräche mit diesen Typen eingelassen, weil man den Verfassungsschutz bespitzeln wollte, ist ebenso absurd wie verlogen. Es ist nichts als eine Schutzbe-

hauptung, mit der sich erfahrungsgemäß aufgeflogene Spitzel von ihrem Verrat rein zu waschen versuchen.

Wenn du angequasselt wirst, hilft nur eines: Sofort abblocken! Fordere die oder den Typen auf, dich in Ruhe zu lassen. Wenn du in dieser Lage nicht so knallhart reagieren kannst, dann sag einfach, dass du jetzt keine Zeit hast. Das hat zwar zur Folge, dass sie dir eine Telefonnummer aufdrängen werden und um Rückruf bitten oder dich ein zweites Mal aufsuchen; aber wenn du auch dann keine Zeit hast und nicht zurückrufst, ist die Sache in der Regel ausgestanden. Schaue dir die drei Minivideos eines versuchten Staatsschutz-Anquatschversuchs in unserem SfN Informationsblog an und verinnerliche die gezeigten Bilder

11.2.4 Anwerbeversuche sofort bekannt machen!

Niemand kann etwas dafür, wenn er vom VS oder der politischen Polizei angequasselt wird. Sie sprechen dich ganz diskret an und tun so, als sei alles ganz vertraulich. Damit wollen diese **Drei - Groschen - James - Bonds** dir das Gefühl geben, dass du besonders von ihnen ausgewählt worden bist.

Diese Situation ist vielen Betroffenen unangenehm und deshalb wollen sie am liebsten niemandem davon erzählen. Schließlich, so beruhigen sie sich selbst, ist ja gar nichts passiert. Doch genau von diesem Schweigen profitieren die Verfolgungsbehörden. Denn wer etwas verheimlicht, spielt schon unbewusst das Spiel dieser geheimen Dienste mit und schützt sogar deren Zuhältertätigkeit. Anwerbeversuche müssen grundsätzlich sofort bekannt gemacht werden! Zumindest im direkten politischen Umfeld, bei deinen vertrauten Personen.

Dadurch erreichst du zweierlei:

Du schützt dich selbst vor Verdächtigungen, weil du den Anwerbern die Chance nimmst, dich später als jemand zu outen, der sich auf Gespräche oder mehr mit denen eingelassen hat.
Du schützt andere Aktivisten (aus deinem Umfeld), weil du sie vorwarnen kannst.

Wenn du eine gute Beobachtungsgabe hast, kannst du die Typen sogar recht gut beschreiben, die dich anwerben wollten. Das schränkt den Wirkungskreis dieser Drei - Groschen - James - Bonds erheblich ein, wenn sie nicht sogar eine weitere Anwerbetätigkeit in deiner Region ganz unterlassen müssen, weil sie „verbrannt“ sind. Warte nicht zu lange, bis du einen Anwerbeversuch bekannt machst! Einen Aktivisten deines Vertrauens oder auch deiner Gruppe solltest du in jedem Fall unverzüglich über den Vorfall informieren. Erstelle unbedingt sofort ein Gedächtnisprotokoll! Du wirst dich später nicht mal an einen Bruchteil dessen erinnern können, was du in den ersten 1-2 Stunden nach dem Vorfall noch in Erinnerung hast. Gerade der visuelle Eindruck ist in der Regel nach 1-2 Stunden wieder verschwunden, also fange mit der Personenbeschreibung als erstes an.

11.2.5 Dein Gedächtnisprotokoll

Was gehört in dein Gedächtnisprotokoll?

Personenbeschreibung! Wie sahen die Typen aus, die mich angequasselt haben?
Wann und Wo hat der Anwerbeversuch stattgefunden?
Mit welchen Namen und als Mitarbeiter welcher Behörde haben sich die Typen vorgestellt?
Welche Begründung haben sie genannt, warum sie gerade mich ansprechen?
Was für Fragen haben sie mir gestellt?
Über wen haben sie mich ausgefragt?
Haben sie versucht, mich unter Druck zu setzen? Wenn ja, womit?
Wie habe ich mich verhalten?
Wie lange dauerte der Vorfall? (zeitlicher Ablauf)

Mit welchem Fahrzeug sind die Typen gekommen? (Kennzeichen?)

Wohin mit deinem Gedächtnisprotokoll?

Protokoll und mündlicher Bericht sofort an Vertrauensperson / Gruppe
Anwerbeversuch mündlich / schriftlich im Umfeld bekannt machen
Protokoll zur Veröffentlichung an Aktionsbüros, Infotelefone, bekannte Weltnetzseiten oder auch Publikationen schicken!
Für Berlin ist es ratsam sich an www.nwbb.org zu wenden.

Du kannst dein Protokoll auch über die Seite SfN Infoblog - Artikel einreichen an uns schicken und wir veröffentlichen das Gedächtnisprotokoll im Blog

11.2.6 Welchen Schaden richten Spitzel an?

Wir haben bereits festgestellt, dass die Verfolgungsbehörden Spitzel brauchen, um an vielschichtige Informationen zu gelangen, aus denen sie Rückschlüsse ziehen können. Gerade psychologisch gesehen sind diese Rückschlüsse für sie wichtig, um immer neue Strategien entwerfen zu können, mit denen sie unsere politische Arbeit und Vorgehensweise behindern und Aktivisten einschüchtern wollen.

Es gibt aber noch andere Bereiche, für die das System Spitzel benötigt. Gerade der Inlandsgeheimdienst „Verfassungsschutz“ hat auch **die Motivation, das Geschehen innerhalb der nationalen Opposition beeinflussen und Menschen kriminalisieren zu können. Dafür stiftet der VS seine Spitzel auch zu kriminellsten Handlungen an und garantiert ihnen dafür Straffreiheit.**

Der VS selbst wird überhaupt nicht belangt, und wenn er Bombenanschläge durchführen lassen würde, die sein „Celler Loch“ noch um ein vielfaches übertreffen. Man sollte daher nicht dem Irrglauben verfallen, dass jemand, der sein Umfeld zu Straftaten anstiftet, gar kein Spitzel sein könne, weil das System so etwas nicht zulassen würde. Das Gegenteil ist der Fall, denn für den staatlich verordneten „Kampf gegen Rechts“ gelten offenbar keine Gesetze mehr.

Spitzel werden dazu angestiftet, kriminelle Handlungen im Umfeld von bestimmten Parteien / Gruppen zu begehen, damit anhand solcher Taten Verbotsgründe gegen diese Strukturen konstruiert werden können.

Beispiel:

Der Verbotsantrag der Schröder-Regierung gegen die NPD fußte im Wesentlichen auf der Wühlarbeit von Spitzeln.

Weiteres Beispiel:

In München hat ein VS-Spitzel die Führungsperson einer größeren Kameradschaft, und damit letztlich die Kameradschaft als solches, negativ beeinflusst. Er bastelte die Legende von einem angeblich geplanten Bombenattentat auf einen J****tempel in der Münchener Innenstadt, die den Staatsbehörden einen willkommenen Vorwand für schwere Repression lieferte.

Das ist eine klassische Vorgehensweise, die immer wieder angewandt wird. Hier hat mal ein Spitzel eine strafbare Rede auf einer Versammlung gehalten, dort hat mal ein Spitzel einen j****chen Friedhof geschändet oder ein Bombenattentat geplant. Solche Straftaten werden dann nationalen Gruppierungen in die Schuhe geschoben, weil es „ihre“ Mitglieder seien. Tatsächlich aber sind

es bezahlte Provokateure des Systems! **Spitzel werden dazu angestiftet, strafbare Musik zu produzieren und einen Verteilerkreis für ihre strafbaren Tonträger aufzubauen. Diesem Verteilerkreis gehören zum größten Teil gutwillige Aktivisten an, die dann später mit Gerichtsverfahren und Gefängnisstrafen überzogen werden.**

Ein Beispiel:

Die Band „White Aryan Rebels“ bestand nur aus einer Person, die alles mit Hilfe von ahnungslosen Musikern eingespielt und anschließend vertrieben hat. Diese Person, Toni Stadler, flog als Spitzel des VS Brandenburg auf!

Spitzel in hochrangigen Parteikreisen werden dazu angestiftet, die Partei dahingehend zu beeinflussen, dass sie ihren politischen Kurs in eine vom System gewünschte Richtung ändert, damit z.B. unnötige Spaltereien aufkommen und die Partei in Flügelkämpfen zermürbt wird. So bringen Überwachungsbehörden über ihre Spitzel Unruhe in die Nationale Opposition, hetzen gutwillige Aktivisten gegeneinander auf, spielen sie nach Belieben aus. Das alles kostet unsere Kraft! Kraft, die uns im politischen Kampf fehlt, weil wir uns viel zu leicht durch Gerüchte und Geschwätze irritieren und von Mackerhaften Selbstdarstellern blenden lassen.

11.2.7 Wie können wir uns schützen?

Über eines müssen wir uns im Klaren sein:
Es hat immer Spitzel in oppositionellen, systemkritischen Bewegungen gegeben und es wird sie auch immer geben.

Je größer eine Bewegung im Laufe der Zeit wird, desto mehr „Strandgut“ wird angeschwemmt. Das braucht uns nicht zu verunsichern und darf auch nicht dazu führen, dass wir die „Schotten dicht machen“. Das wäre genau die Reaktion, die das System mit seinen Zersetzungsbemühungen erreichen will. Der nationale Widerstand muss offen bleiben für neue Menschen, die zu uns stoßen wollen. Was sich ändern muss, damit wir uns vor Bespitzelung und Kriminalisierung wirksamer schützen können, sind die Maßstäbe, mit denen wir die Personen in unserem Umfeld beurteilen. Man kann einen Spitzel zwar nicht an der Nasenspitze erkennen, aber man kann es einem Spitzel sehr schwer machen, seine Wirkung zu entfalten, wenn man einige grundlegende Dinge beachtet:

Eigene Disziplin: Reduziert eure politischen Gespräche am Telefon auf ein notwendiges Minimum. Das gleiche gilt auch für Post, eBriefe und Weltnetz. Benutzt Verschlüsselungsprogramme zur Nachrichtenübermittlung. Sprecht nicht in Gegenwart von Unbekannten oder Außenstehenden über interne Dinge.

Schluss mit der Naivität: Nicht jeder „Neue“ ist gleich ein Kamerad! Beobachtet euren Zuwachs ausgiebig und lasst ihn keine Einsicht in eure internen Abläufe / Aufgabenverteilungen haben.

Ein guter Gruppenführer sollte mindestens zweimal bei einem „Neuen“ in der Wohnung gewesen sein: Einmal angemeldet und einmal unangemeldet!

Überprüft seine Vergangenheit und alten Arbeitsstellen. Ruft gegebenenfalls dort an. Recherchiert, ob seine Angaben stimmen.

Bewertet Personen in eurem Umfeld nie nach ihren Worten, sondern nur nach ihren Taten! Wer viel schwätzt und wenig tut, sollte aus Sicherheitsgründen von allen wichtigen Besprechungen und Informationen ferngehalten werden.

Das gleiche gilt auch für labile, charakterschwache, erpressbare Personen: Je weniger sie über interne Angelegenheiten erfahren, desto geringer ist die Chance, dass sie im Falle einer erfolgreichen Anwerbung durch VS und Polizei Schaden anrichten können. Wer andere Aktivisten zu erkennbar strafbaren Taten anstiftet, muss sofort aus eurem Umfeld aussortiert werden! **Gerade bei klischeehaften Straftaten (Ausländer aufmischen, Asylantenheime anzünden, j****che Friedhöfe schänden) sollten bei jedem verantwortungsbewussten Aktivisten sämtliche Alarmglocken schrillen! Solche Taten haben nichts mit unserem politischen Kampf zu tun und sind außerdem kontraproduktiv.**

Ein aktuelles Beispiel:

Mit großem Mediengetöse wurde Stephan Michael Bar im Jahr 2001 als ein „Top-Aussteiger“ aus der Neonaziszene gefeiert. Zuvor wurde er von vielen unkritischen Aktivisten lange Zeit als „Kamerad“ angesehen, „prominent“ aufgrund seiner medienwirksamen Straftaten noch dazu. Kaum einer wollte wahrhaben, was bereits lange vor Bars „Ausstieg“ schwarz auf weiß zu lesen war: Bar hatte umfangreiche Aussagen bei der politischen Polizei (LKA) gemacht und dabei Aktivisten aus seinem Umfeld verraten, um seine persönliche Haftsituation zu verbessern.

Vorsicht bei Personen, die Waffen in der Szene etablieren wollen und vom bewaffneten Kampf faseln, der schon bald beginnen müsse. Wer so agiert, spielt dem Staat in die Hände, egal ob er Spitzel ist oder nicht. Personen, die immer wieder Unruhe stiften und nutzlose Spaltereien in eurem Umfeld betreiben, sollten zügig aussortiert werden. Selbst wenn sie niemals als Spitzel auffliegen sollten, sind sie dennoch Schädlinge, die zumindest von der Geisteshaltung her Spitzeln gleich sind.

11.2.8 Wenn Spitzel fliegen lernen...

In der letzten Zeit hat das System verstärkt Spitzel auffliegen lassen. Nach Außen hin mag das wie zufällig erscheinen oder wird der Recherchearbeit etablierter Magazine (Spiegel, Focus) zugeschrieben. **Tatsächlich jedoch werden Spitzel von ihren geheimdienstlichen Zuhältern bewusst „verbrannt“.**

Den Medien werden die gewünschten Informationen zugespielt, sofern dies nötig ist. Man darf aber davon ausgehen, dass in den Redaktionsstuben etablierter Medien genügend Informanten der Geheimdienste sitzen, über die das Auffliegen lassen von Spitzeln lanciert wird. Bei jedem Spitzel kommt früher oder später der Zeitpunkt, wo er für seine Zuhälter beim VS, LKA, BKA, MAD nicht mehr von Nutzen ist. Dann wird er „abgeschaltet“.

Damit ist die Sache aber keinesfalls ausgestanden, denn der abgeschaltete Spitzel wird immer mit der Ungewissheit leben müssen, dass er aus taktischen Gründen auch Jahre später noch als enttarnter Spitzel ans Licht der Öffentlichkeit gebracht wird. Und das ist auch gut so. Das System hofft, durch solche Spitzelenthüllungen den nationalen Widerstand verunsichern zu können. Wir sollen das Vertrauen in unsere Mitkämpfer verlieren, denn jeder von ihnen könnte der nächste Spitzel sein.

Es kommt für uns also darauf an, einen konsequenten Umgang mit Spitzeln zu finden, um Verunsicherung und Misstrauen in unseren Reihen entgegenwirken zu können. Hysterie und vorschnelles Verurteilen ist dabei genauso wenig angesagt, wie Gleichgültigkeit und Schweigen. Wir müssen mit dem Bewusstsein, dass sich Spitzel in unserem Umfeld herumtreiben, gelassen und unbeirrt weiter arbeiten können.

Wenn aber einer als Spitzel enttarnt und zweifelsfrei überführt ist, dann muss für alle sichtbar die Konsequenz gezogen werden!

11.2.9 Die einzige Konsequenz: Null Toleranz!

Bei den Spitzelenthüllungen im Zuge des NPD - Verbotsverfahrens - aber nicht nur dort - hat sich gezeigt, wie windelweich und fahrlässig bestimmte Teile der nationalen Opposition mit Verrätern umgehen.

Ein Beispiel:

Da hat der NPD-Funktionär Wolfgang Frenz aus NRW über Jahrzehnte seine Parteigenossen ausspioniert und dann wird er nach seiner Enttarnung sogar noch in pseudonationalen Kreisen wie ein Promi hofiert. So geschehen im Rahmen einer Saalveranstaltung des NPD-Mitgliedes Günter Deckert in Heidelberg, wo Frenz ganz locker über seine Spitzeltätigkeit plaudern durfte.

Weiteres Beispiel:

Der im Jahre 2001 enttarnte Spitzel Tino Brandt, der rund sieben Jahre für den VS Thüringen arbeitete, wird bis heute nicht konsequent geächtet. Vor laufender Fernsehkamera zeigten sich „Kameraden“ aus seinem Umfeld sogar solidarisch mit dem homosexuellen Falschspieler, der sich von seinen Spitzelgagen ein nettes Häuschen mit Garten zugelegt hatte. Öffentliche Ächtungsbekundungen suchte man damals in Thüringen vergeblich, weil die Kameraden im Umgang mit diesem Problem überfordert waren. Stattdessen wurden in der „Szene“ Interviews mit Tino Brandt geführt, die dann von diversen Publikationen unkritisch und gedankenlos abgedruckt worden sind.

Die Ausreden von Leuten, die enttarnte Spitzel in Schutz nehmen, sind genauso so erbärmlich, wie die Ausreden der Spitzel, warum sie jahrelang für den Feind gearbeitet haben. Es gibt keine Rechtfertigung für eine Zusammenarbeit mit dem Feind und es gibt keine Rechtfertigung dafür, einen erkannten Spitzel weiterhin in nationalen Zusammenhängen zu dulden.

Wer sich für dieses System prostituiert, stellt sich außerhalb unserer Gemeinschaft, weil er die Grundlagen, auf denen unsere Gemeinschaft basiert, mit Füßen tritt. Zu diesen Grundlagen gehören gegenseitiges Vertrauen, Aufrichtigkeit und die politische Einsicht, dieses System konsequent abzulehnen. Wer aber spitzelt, macht sich zu einem Teil des Systems. Wer spitzelt, akzeptiert Lüge und Verrat und nimmt sich damit selbst die Ehre. **Für ehrlose Lumpen aber ist bei uns kein Platz!**

Daher: Seht nicht schweigend zu, wenn ein Spitzel aus eurem Umfeld enttarnt wurde, sondern geht in die Offensive! Jeder mediengerechten Enttarnung muss sofort eine öffentliche Ächtung durch uns folgen, damit klare Verhältnisse geschaffen werden. Wir erreichen damit, dass:

enttarnten Spitzeln ein Verbleib in ihrem gewohnten Umfeld oder das Einnisten in einem neuen Umfeld spürbar schwerer oder besser noch unmöglich gemacht wird!

der Wirkungskreis von bislang nicht enttarnten Spitzeln eingeschränkt wird, weil sie Angst vor den Konsequenzen einer Enttarnung haben müssen!

wir nach Innen wie nach Außen durch eine kompromisslose eindeutige Vorgehensweise unsere politische Glaubwürdigkeit als Systemablehnende Opposition bewahren.

Schaffen wir gemeinsam ein Klima der Ächtung und Ausgrenzung gegenüber Spitzeln und brandmarken wir konsequent auch jeden, der sich dieser Selbstverständlichkeit widersetzt!

11.3 Verhalten bei Demonstrationen

Allgemeine Informationen

Diese Seiten sollen dir als Ratgeber im Umgang mit verschiedenen Situationen bei Demonstrationen dienen. Jeder ist gehalten, durch persönliche Gespräche und einen lebendigen Erfahrungsaustausch zur Schulung seiner Kameraden beizutragen. Jedoch sollten „Ammenmärchen“ und Schaudarstellungen vermieden werden: Letztendlich geht es nicht darum, kriminell zu werden, sondern gesetzlich verbriefte Rechte wahrzunehmen, um dem politischen Ziel ein Stück näher zu kommen.

Hierbei sollten gerade die jungen Kameraden in realistischer Weise an die Möglichkeiten politischer Wortergreifung in der Öffentlichkeit herangeführt werden - diese bringen mehr, als Provokation, Gewalt oder Selbstdarstellerei es jemals könnten. Es geht nicht darum, die „coolste Randgruppe“ zu verkörpern, sondern vereint wieder die Mitte des Volkes zu werden!

Generell gilt: (laut Grundgesetz Artikel 8)

Alle Deutschen haben das Recht, sich ohne Anmeldung oder Erlaubnis friedlich und ohne Waffen zu versammeln. Für Versammlungen unter freiem Himmel kann dieses Recht durch Gesetz oder auf Grund eines Gesetzes beschränkt werden.

Das bedeutet, dass wir erstmal demonstrieren dürfen. Jedoch machen verschiedene Vorschriften, wie z.B. das Versammlungsgesetz weitere Einschränkungen. Das bedeutet u.a. dass die Veranstaltung ordnungsgemäß angemeldet sein muss und die Teilnehmer sich friedlich verhalten (keine Angriffe gegenüber Personen (Passanten, Gegen-Demonstranten, Polizisten usw.) oder Objekten).

11.4 Verhalten bei einem feindlichen Outing

Immer wieder sind nationale politische Aktivisten durch sog. „Outings“ von Linksextremisten betroffen. Die Folgen können weitreichender sein, als es auf den ersten Blick scheint. Grund genug, sich damit zu befassen, ob und was sich im Vorherein bzw. Nachhinein dagegen tun läßt.

Feindliche „Outings“ zielen immer darauf ab, den Betroffenen angreifbar zu machen. Natürlich wissen auch Linksextremisten, daß sie mit ihren Flugblättern und Schmierparolen nur selten die Nachbarschaft gegen uns aufbringen können. In der Regel passiert eher das Gegenteil: Viele Nachbarn solidarisieren sich mit Betroffenen und bringen zum Ausdruck, daß sie die Stasi- Methoden der linksextremen Hetzer verabscheuen. In nahezu allen uns bekannten Fällen der letzten Jahre kam es durchweg zu positiven Reaktionen. Das ist die gute Nachricht.

Es gibt aber auch eine schlechte: Das Ziel des feindlichen „Outings“ ist sowieso ein ganz anderes. Es geht nämlich darum, den potentiellen Täterkreis unüberschaubar groß zu machen. Meist fängt es auf einschlägigen Feindseiten im Internet an, daß Name und Wohnanschrift sowie weitere persönliche Daten des Betroffenen verbreitet werden. Dann folgen Flugblätter und Schmierparolen im Wohnumfeld, ggf. auch beim Arbeitgeber oder beim Sportverein oder wo auch immer der Betroffene sich privat regelmäßig aufhält. Durch diese Vorgehensweise wird der Kreis derjenigen, die über die Aktivitäten des Geouteten informiert sind, immer größer. Das erschwert später ganz erheblich die Ermittlungen der Polizei, sobald es mit Anschlägen und gewaltsamen Überfällen los geht. Es läßt sich nicht mehr so einfach eingrenzen, aus welcher Ecke die Täter kommen könnten.

Wie diese feindlichen „Outings“ ablaufen wurde schemenhaft durch die „FAZ“ beschrieben:

... Noch in derselben Nacht wird die Nachricht ins Internet gestellt: „Florian W. geoutet“, steht auf der Internetseite „Indymedia.org“. Dort wird spekuliert, auf welchen Demonstrationen Florian W. sonst noch gesehen worden ist. Es werden weitere Bilder ins Netz gestellt; auch solche, von denen selbst der Einsteller nicht sicher ist, ob es sich überhaupt um Florian W. handelt. Am nächsten

Morgen klingelt bei Florian W. das Telefon. Im Internet heißt es wenig später dazu, man habe soeben einen „Testanruf“ gemacht - und herausgefunden, dass Florian W. noch bei seinen Eltern wohnt.

An die Telefonnummer ist der Anrufer über das Flugblatt gelangt. Denn sowohl die Festnetz- als auch Handynummer sind in dem Steckbrief veröffentlicht. Ebenso wie Geburtsdatum, ICQ-Nummer, SchülerVZ-Account und sein Name bei „Wer kennt wen“. Es ist kurz nach zwei Uhr morgens in der Nacht zu Heiligabend, als Florian W. zu einer öffentlichen Person wird.

(Den ganzen Artikel kannst du in der Frankfurter Allgemeine Zeitung lesen.)

Doch was kann man tun gegen ein „Outing“? Läßt es sich verhindern?
Und was, wenn das „Outing“ doch passiert ist?
Wie sieht es eigentlich rechtlich aus?
Was kommt nach dem „Outing“ ?
Nachwort

Weitere Informationen zum Thema Feindliches Outing findest du im SfN Infoblog:
www.blog.s-f-n.org/tag/outing
Grund ihrer beruflichen Situation anvertraut oder bekannt geworden sind.

Nach § 53a StPO steht dieses Recht auch den Berufshelfern der genannten Personen zu. Unter den Voraussetzungen des § 55 StPO heißt das Aussageverweigerungsrecht. Es steht allen denjenigen zu, die durch wahrheitsgemäße Beantwortung von Fragen sich oder einen Verwandten oder Verschwägerten (§ 52 StPO) der Gefahr strafrechtlicher Verfolgung aussetzen würden.

Das Strafprozessrecht verbietet, aus dem berechtigten Schweigen eines Beschuldigten oder Zeugen nachteilige Folgerungen zu ziehen. Wenn du auch ohne gesetzliche Berechtigung nicht bereit bist, gegen Volksgenossen oder Kameraden auszusagen, kann es dir im schlimmsten Fall passieren, dass du für 6 Monate in Beugehaft genommen oder zu einer Geldstrafe verurteilst wirst. Bereits aus dem Wortlaut dieser Gesetzesvorschriften ergibt sich, dass die Rechte eines Beschuldigten oder Zeugen für die Ermittlungsbehörden Hindernisse darstellen, die sie gerne überwinden wollen. Sie werden sich oft genug vorkommen wie jemand, der den Saft einer Zitrone haben will, sie aber nicht verletzen darf. Sie werden also versuchen, den Verdächtigten oder den schweigeberechtigten Zeugen dazu zu bringen, sein Schweigen aufzugeben und sich zu äußern. Den Ermittlungsbeamten, meist Kriminalbeamten, steht hierfür ein großes Instrumentarium an psychischen und physischen Beeinflussungsmitteln zur Verfügung, dessen Betätigung sie gelernt haben. Dies beherrschen sie und wissen damit umzugehen.

11.4.1 Die Vermischung legaler und illegaler Methoden

Die Erfahrung hat gezeigt, dass der ausführliche Katalog des § 136 StPO die Vermischung legaler Praktiken mit illegalen Praktiken nicht ausschließt. Die Grenze zu ziehen zwischen Ermüden und Wachsein, zulässiger Qual und unzulässiger Quälerei, die Bestimmung dessen, was Täuschung oder ein gesetzlich nicht vorgesehener Vorteil ist, dürfte im Einzelfall kaum möglich sein.

Hinzu kommt, dass die Beamten meist sehr genau wissen, was sie sich leisten können und wann eine rechtswidrige Vernehmungsmethode als solche erkennbar ist. Sie werden dies nur so weit tun, als es ihnen nicht bewiesen werden kann. Übrigens reichen auch die zulässigen Methoden in ihrer psychischen und physischen Wirkung aus, einen ungeübten, nicht gewappneten Menschen fertigzumachen.

Es ist daher müßig, sich in diesem Zusammenhang lange bei der Unterscheidung von legal und illegal aufzuhalten. Wenn man weiß, was einen erwartet, ist man am ehesten in der Lage, seine

„Willensbetätigung“ zu beherrschen und seine Rechte zu wahren

11.4.2 Dein Recht auf Aussageverweigerung

Beachte bitte das Kapitel: Aussageverweigerung

Eine Festnahme, ein Verhör oder eine Hausdurchsuchung trifft dich fast immer unvorbereitet. Das gehört bereits zur erfolgsgerichteten Taktik der Polizei. In dieser Situation hat sie dir gegenüber folgende Vorteile:

Für dich ist diese Situation eine Ausnahme - für sie ist es eine Routine.
Du bist von Personen deines Vertrauens abgeschnitten.
Die Beamten haben ständig die Möglichkeit, bei veränderter neuer Lage neue Instruktionen einzuholen.
Du kennst deine Rechte nur unvollkommen, sie wissen das.
Du bist nervös und aufgeregt. Sie sind gelassen und darauf getrimmt, deine Nervosität zu ihren Gunsten auszunutzen.
Du weißt nicht, was sie mit dir machen werden und wie lange das Verhör dauert und was es ergibt - sie haben davon eine genaue Vorstellung.
Du bist ausgeliefert und fühlst dich entsprechend schlecht.
Die Angst und die Ungewissheit machen dich fertig - sie rechnen damit.

In dieser Situation sind viele bereit, auf alle gesetzlich garantierten Rechte, im besonderen auf Aussageverweigerung, zu verzichten. Für den Wunsch „nur raus hier und es hinter mir haben“, sind manche schon für Jahre ins Gefängnis gewandert, weil sie ihr Recht auf Schweigen nicht mehr wahren konnten. In dieser Lage bist du nicht Herr des Verfahrens. Du kannst mit absoluter Sicherheit nicht wissen, ob eine Aussage deine Situation letztendlich verbessert. In dieser Lage kannst du nur spekulieren.

Spekulation ist Abenteurerei
Es gibt keine Situation, in der du eine Aussage nicht auch noch in 14 Tagen machen könntest!
Wichtig ist, die Mechanismen zu kennen, die Menschen zum Reden bringen. Eine Vernehmung ist kein Spiel von Frage und Antwort. Sie ist zunächst eine Situation, in der man nicht nur bewusst und vernünftig handelt, sondern vor allem von unbewussten Regungen, teilweise mechanisch, gesteuert wird. Der geübte Kriminalbeamte wird, wenn der dich schon kennt, bereits von Anfang an diese Regungen und Verhaltensweisen an dir studieren. So kann er im Verlauf der Handlungen in deinem Unterbewusstsein Reaktionen auslösen, die ihn seinen Zielen näher bringen. Viele begreifen später nicht, wie es zu Aussagen kommen konnte.

Warum ist es richtig, nichts zu sagen, bevor man nicht mit seinem Anwalt gesprochen hat?

Das Gesetz gibt dir als Beschuldigter das Recht, dich selber nicht zu belasten. Das gleiche gilt für den Zeugen unter den oben genannten Voraussetzungen. Es gibt vor allem nach einer Festnahme keine Situation, in der du sachlich und juristisch beurteilen kannst, ob deine Angaben tatsächlich einen Vorteil für dich bringen. Du weißt gar nicht, an welcher Stelle des Verfahrens du bist. Dir fehlt der Lotse. Frag erst einen Anwalt! Wenn er nicht erreichbar ist, warte mit allem, bis du ihn erreicht hast und er kommen kann. Mach dir unter keinen Umständen die Ungeduld und Eile des Beamten zu eigen. Wenn er es eilig hat, hast du gerade Zeit. Und nimm bloß nicht ihn etwa als Lotsen. Du kannst dir hoffentlich denken, dass er dich nicht in deinem Interesse, sondern in seinem lotst.

Der Polizeibeamte hat nur ein Ziel: Seinem Vorgesetzten ein Ergebnis zu präsentieren. Du bist ihm letztlich scheißegal! Wenn du aufgrund deiner Aussage noch im Knast sitzt, ist er dafür vielleicht

schon befördert worden.

11.4.3 Warum ist es wichtig, mit einem Anwalt zu sprechen

Das Gesetz gibt dir als Beschuldigten das Recht, dich selber nicht zu belasten. Das gleiche gilt für den Zeugen unter den oben genannten Voraussetzungen. Es gibt vor allem nach einer Festnahme keine Situation, in der du sachlich und juristisch beurteilen kannst, ob deine Angaben tatsächlich einen Vorteil für dich bringen. Du weißt gar nicht, an welcher Stelle des verfahrens du bist. Dir fehlt der Lotse. Frag erst einen Anwalt

Wenn er nicht erreichbar ist, warte mit allem, bis du ihn erreicht hast und er kommen kann. Mach dir unter keinen Umständen die Geduld und Eile des Beamten zu eigen. Wenn er es eilig hat, hast du gerade Zeit. Und nimm bloß nicht ihn etwa als Lotsen! Du kannst dir hoffentlich denken, dass er dich nicht in deinem Interesse, sondern in seinem lotst.

11.4.4 Die prozessuale Bedeutung der Aussageverweigerung

Dein Schweigen hat auch prozessuale Bedeutung. Nur die totale Aussageverweigerung darf bei einem Beschuldigten nicht zu seinem Nachteil gewertet werden. Sagst du nur ein Wort, so wird dies zu einem Beweismittel, das nach der Rechtssprechung der tatrichterlichen Beweiswürdigung unterliegt.

Beispiel:

Du wirst gefragt, wo du im August 1998 warst. Wenn du bisher weder auf diese noch auf eine andere Frage geantwortet hast, kann dein Schweigen nicht verwertet werden. Sagst du aber nur: „Am 17.August habe ich demonstriert“ (vielleicht, weil man dir ein Foto vorhält, auf dem du zu sehen bist), so kann daraus der Schluss gezogen werden, dass du an diesem oder jenem Ort warst und dieses oder jenes getan hast.

Also:

Solange du keinen Lotsen hast: SCHWEIGEN! Eine Aussage kann man nicht widerrufen. Man kann nur einer Aussage eine weitere hinzufügen, die vom Inhalt der Ersten abweicht. Das Gericht ist dann in seiner Wertung frei, welcher es Glauben schenkt. Meist werden die Beamten, welche die Aussage zustande gebracht haben, in der Verhandlung vernommen, und die werden ihr übriges tun, die geeignete Aussage dem Gericht mundgerecht zu machen.

11.4.5 Die Spekulation mit deiner Angst

Ein wesentliches Instrument deiner Gegner mit dem sie versuchen dich kleinzukriegen ist es dir Angst zu machen. Angst hat vor allem derjenige, der zu weiterem Widerstand keinen Mut mehr hat. Dieser Mut verlässt einen, wenn der Gegner einem übermächtig erscheint. Es gehört somit zur Taktik der Polizei, dir zu zeigen, dass Widerstand sinnlos ist und dass man mit dir machen kann, was man will.

Dass keiner deine Schreie hört, wenn du geschlagen wirst. Du fühlst dich machtlos wie ein Stück **Knete. Vergiss aber nicht, dass du keine Knete bist! Du bist ein Freiheitskämpfer und durchschaust das Manöver. Das zeigst du aber keinem.**

Es ist vor allem das Imponiergehabe der Polizei bei deiner Festnahme, deiner Hausdurchsuchung oder bei anderer Gelegenheit, das dich mutlos machen soll:

Jeder weiß, dass die Polizei nicht bei Nacht in die Wohnung kommen darf und schon gar nicht ohne richterlichen Befehl (§§ 104, 105 StPO). Die Polizei setzt sich über diese Vorschriften hinweg,

indem sie die in diesen Vorschriften vorgesehenen Ausnahmen zur Regel macht. Sie zeigen dir, dass sie sich das und noch viel mehr leisten können. Du kannst dich ja beschweren (Hohngelächter). Sie demonstriert Sicherheit.

11.4.6 Hausdurchsuchungen

Beachte bitte das Kapitel: Hausdurchsuchungen

Rechtsgrundlage für Hausdurchsuchungen sind die §§ 102 ff. StPO. Diese Vorschriften schränken das in Artikel 12 des Grundgesetzes garantierte Grundrecht auf Unverletzlichkeit der Wohnung ein. Das Gesetz regelt ausführlich, wann und unter welchen genau beschriebenen Bedingungen in dieses grundsätzlich geschützte Rechtsgut eingedrungen werden darf:

- Nur auf richterliche Anordnung. Lediglich bei Gefahr im Verzug auch auf Anordnung der Staatsanwaltschaft oder bestimmter Kriminalbeamter (§ 105 StPO);
- Nachts darf dies nur bei Verfolgung auf frischer Tat oder bei Gefahr im Verzug angeordnet werden (§ 104 StPO);
- Wenn kein Richter oder Staatsanwalt der Durchsuchung beiwohnt, so sind wenn möglich ein Gemeindebeamter oder zwei andere neutrale Zeugen zuzuziehen (9105 Abs. 2 StPO);
- Eine Durchsicht der Papiere des von der Durchsuchung Betroffenen steht nur dem Richter zu, es sei denn, der Betroffene ist mit der Durchsicht durch andere einverstanden (§ 110 StPO).

Für den normalen Recht empfindenden Bürger, der keine einschlägigen Erfahrungen hat, liest sich das Gesetz wie ein Katalog von rechtsstaatlichen Garantien zur Wahrung seiner Wohn - und Lebenssphäre als Schutz vor polizeistaatlichen Eingriffen.

Bestimmte Gesetzestexte sind reine Justizpropaganda. Mit ihnen soll bei allen, die es lesen, der Glaube an die heile Justizwelt erhalten werden. Jeder der Erfahrungen mit Hausdurchsuchungen hat, weiß, dass die Praxis anders aussieht.

Die Ermittlungsbehörden bedienen sich dabei des Begriffes der „Gefahr im Verzug“. Was vom Gesetzestext her als Ausnahme formuliert ist, wird in der Praxis zur Regel. Ohne im Einzelnen näher zu begründen, woran die Gefahr zu sehen ist, wird unter Umgehung von Gericht und Gesetz in vielen Fällen so verfahren, als gäbe es weder Gesetz noch StPO.

Der Rechtsbegriff „Gefahr im Verzug“ wird zur leeren Legitimationsfloskel für rechtswidrige Ermittlungsmethoden:

- Beschwerde gegen die Hausdurchsuchung einzulegen ist sinnlos, weil sie keine aufschiebende Wirkung hat. Da aber das Gericht erst entscheidet, wenn die Beamten längst über alle Berge sind, ist die Beschwerde gegenstandslos. Eine beendete Maßnahme lässt sich nicht mehr verhindern.
- Eine Strafanzeige gegen die verantwortlichen Beamten etwa wegen Hausfriedensbruch im Amt oder wegen Nötigung ist sinnlos. Die Anzeige wird von der Staatsanwaltschaft und der Kripo bearbeitet. Selbst wenn ein rechtlich denkender Staatsanwalt oder Kriminalbeamter diese Methoden für ungesetzlich halten sollte, so wird dieser doch nicht gegen seinen Chef, der wieder einen Chef hat, ein Verfahren durchsetzen können.

11.4.7 Erfahrungsprotokoll - Eine Hausdurchsuchung

Ich wache auf, weil jemand an der Tür rüttelt. Ich denke: Einbrecher! Dann ein kurzes Klingeln und ehe ich ganz wach bin und aufstehen kann, sind sie schon da. Ein Rollkommando der Polizei mit Maschinenpistolen im Anschlag stehen um mein Bett herum. Sofort fallen mir Zettel ein, Adressenlisten, Bücher, die verboten sein könnten. Immer dieses verdammte schlechte Gewissen. Sehe ich einen Polizisten auf mich zukommen, überlege ich sofort, ob ich irgend etwas falsch gemacht haben könnte. Vielleicht sind wieder Schriften von Zündel oder Walendy verboten worden - einen Moment scheint mir alles möglich. Dann komme ich wieder zu mir und frage, warum sie bei mir Hausdurchsuchung machen.

„Hier sind wir es, die Fragen stellen, das werden sie schon früh genug erfahren."

Nun möchte ich den Durchsuchungsbefehl sehen. „Durchsuchungsbefehl?", sagt einer höhnisch, „den brauchen wir nicht, Gefahr im Verzug." Einer bewacht das Telefon, und als ich verlange mit meinem Anwalt zu telefonieren, heißt es „das könne ich später tun". Sie benehmen sich so, als ob ich froh sein müsste, von ihnen überhaupt eine Antwort zu erhalten.

Jeder einzelne von ihnen ein kleiner Machthaber. Aber wahrscheinlich haben sie selber Angst, vermuten ein Waffenlager oder so etwas, fühlen sich in Feindesland. Als würden sie erwarten, dass ihnen jeden Augenblick ein Partisan in den Rücken springt. Sie holen alle Bücher aus den Regalen herunter, wühlen in Zeitschriften, in Archiven, alten Fotomappen, persönlichen Briefen. Der Herr in Zivil, wohl der Staatsanwalt, will wissen, wer denn das auf dem Bild sei, von wem ich denn so viele Briefe bekomme. Als er keine Antwort bekommt, zeigt er auf die Tür eines etwas abgelegenen Zimmers, in dem eine Freundin wohnt, deren Namensschild auch an der Tür hängt. Er fragt, wessen Zimmer das sei. Ob er darauf eine Antwort erwartete weiß ich nicht. Jedenfalls wollen sie mir jetzt wohl zeigen, was eine Harke ist. Sie brechen auch dieses Zimmer auf, reissen überall die Laken aus den Betten, heben die Matratzen hoch, zerren die Platten aus den Hüllen, in der Küche das ganze Geschirr aus den Regalen, das Besteck dazu und kippen zur Krönung noch Marmelade drüber. Sie stampfen durch die Wohnung, als wären sie hier zu Hause und machen einen Lärm, dass mir Angst und Bange wird. Die Nachbarn könnten sich aufregen und der Hauswirt uns kündigen. Endlich sind sie fertig. Ich bestehe darauf, dass ein Protokoll gemacht wird und bin froh, als sie wieder weg sind.

Kurzum:

Die Polizei stürmt deine Wohnung bei Tag und Nacht, wie und wann sie will. Gefahr im Verzug ist immer. Zeugen sind „leider" nie erreichbar. Anwalt? Was wollen sie denn mit dem? Hilft nur noch eins: Die ganze Aktion wie einen Heuschreckenschwarm über sich ergehen lassen, damit der Schaden möglichst gering bleibt. Das kostet Nerven. Diesen Aufwand an Angst und Nervenkraft kannst du gering halten, wenn du folgendes berücksichtigst:
Es gehört zur Taktik der Polizei, Durchsuchungen zu einer Zeit durchzuführen, in der du am wenigsten damit rechnest und am wenigsten widerstandsfähig bist.

Auf diese Weise erhofft man sich Angstreaktionen von dir, die als Ermittlungshinweise für die Polizei wertvoll sein könnten. Also kommt man am frühen Morgen vor dem Aufstehen. Es klingelt oder klopft an der Tür zu einer Zeit, in der nur gute Bekannte zu dir wollen. Die Beamten stürzen schwer bewaffnet in unbegreiflichen Mengen an dir vorbei und besetzen alle Räume in der Wohnung. Du siehst Uniformen neben deinem Bett, Maschinenpistolen in der Küche, und wenn du aufs Klo willst, musst du erst einen Beamten verscheuchen. Deine Wut wird durch deine Ohnmacht gesteigert. Deine Hilflosigkeit macht dir Angst. All diese Reaktionen stärken die Gegenseite. Mach dich von deinem inneren Zwang frei, indem du Widerstand leistest. Äussere Empörung über Zweck und Recht der Aktion. Auch hier gilt: Nichts sagen! Auch wenn man die Aktion dadurch verlängert, du bist rechtlich nicht verpflichtet zu helfen. Am besten ist, wenn du dir in einer ruhi-

gen Stunde mal überlegst, wie du im Falle einer Durchsuchung reagierst. Dann bist du mindestens gedanklich darauf vorbereitet und kannst dich zu einer angemessenen Reaktion zwingen, da du nicht lange nachzudenken brauchst. Versuche so zu reagieren, als geschehe das jeden Tag. Gib den Beamten nicht die Gelegenheit, sich daran zu weiden, wie du dich vor ihnen in deinem Bett oder Nachtgewand schämst. Wenn sie schweinische Bemerkungen machen, so gehe nicht darauf ein. In diesem Sadismus legen sie es oftmals gerade darauf an, dich zu provozieren. Gib ihnen nicht die Ehre, in diesem provozierenden Spiel ihr Partner zu sein. Betrachte sie wie geschlechtslose Wesen, vor denen sich zu schämen überflüssig wäre. Womöglich ist es gerade ihre Angst vor dieser Geschlechtslosigkeit, die sie mit ihren Provokationen töten wollen. Du bist der Überlegene, wenn du dich nicht darauf einlässt. Geh in die Küche und koche dir einen Kaffee. Versuch nicht etwas „zu retten“. Das geht meistens schief. Auf solche Reaktionen ist die Polizei vorbereitet. Darin hat sie Erfahrung. Das lernt sie bereits auf der Polizeischule. Nach zwei Stunden spätestens sind sie wieder weg. Dann ist der Spuk vorbei und du bist eine Erfahrung reicher.

Allerdings ist für deine persönliche Ruhe einiges zu beachten:
Verliere nie den Überblick über Sachen, die in deiner Wohnung sind.
Bewahre keine Sachen auf, die nicht unbedingt für dich von Bedeutung sind.
Lege keine Korrespondenzarchive an.
Mach dich frei von Souvenir- und Dokumentenfetischismus.

Es gibt Kameraden, die schon jetzt dafür arbeiten, dass die spätere Geschichtsforschung möglichst lückenlos Material über unsere Aktivitäten erhält. Wer Adressen, Waffen usw. in seiner Wohnung aufbewahrt, zeigt damit, dass er nur noch in einer Hinsicht ernst zu nehmen ist:

Als Gefahr für seine Kameraden und sich selbst.

Hausdurchsuchungen kommen plötzlich. Sie kündigen sich nicht durch Sternzeichen und andere geheimnisvolle Zeichen an. Lass dich nicht überreden, für Unbekannte oder „gute Freunde“ Sachen in deiner Wohnung unterzustellen, von denen du nicht beurteilen kannst, wozu sie gut sind oder woher sie stammen. Nicht selten folgt solchen Provokationen die „fündige Hausdurchsuchung“ auf dem Fuße. Das ganze klingt, als sei das Ertragen einer Hausdurchsuchung ein Kinderspiel. Das ist es ganz bestimmt nicht. Kaltschnäuzigkeit und besonnen zu bleiben kostet eine Menge Energie. Es ist nicht einfach, wenn du zusehen musst, wie die Beamten mit zynischen Bemerkungen deine Sachen durchschnüffeln, oder wie sie Sachen behandeln, die dir wertvoll sind. Sie werfen deine Bücher auf die Erde und schütteln sie, dass die Seiten fliegen. Es ist vorgekommen, dass sie Lebensmittel auf den Fußboden ausschütten. Wer sich später dagegen erfolgreich zur Wehr setzen will, ist meist in Beweisschwierigkeiten. Sieh zu, dass es Leute gibt, die wissen in welchem Zustand deine Wohnung sich gewöhnlich befindet und wie aufgeräumt sie ist.

Wenn Du Kinder hast, überlege dir jetzt schon einmal, was du mit ihnen tust, falls die Polizei kommt. Die Angst, in so einem Fall allein zu sein oder nicht zu wissen wohin, stärkt die Gegenseite gewaltig. Die Polizei kommt manchmal mehrmals hintereinander, weil sie denkt, man sei so blöd und hole nach überstandener Gefahr jetzt all die gesuchten Sachen hervor. Auch das ist Routine und darf dich nicht aus der Fassung bringen

11.4.8 Festnahmen

Bei Festnahmen erscheint meist ein Polizeiaufgebot in einer Stärke und Bewaffnung, die die Aktion für dich unübersehbar und undurchschaubar macht. Das soll dir den Eindruck vermitteln, man hätte derart viele Erkenntnisse über Deine Gefährlichkeit, dass man dich eigentlich auf der Stelle erschießen könnte. Mancher hat sogar die Beobachtung gemacht, dass die Beamten provozierend am Abzug der Waffe spielten. Dir fällt dann ein, dass du ja nicht der erste wärst, der bei so einer Situation auf der Straße stirbt. Die Angst, die du dann hast, ist wohl berechtigt, aber von den Anderen genau einkalkuliert.

Ein Polizist, der seine Finger am Abzug nicht beherrschen kann, wird erfahrungsgemäß nach aussen hin abgeschirmt. Die Pressepolitik der Polizei ist geschickt genug, um mit einigen in Kauf genommenen kritischen Abstichen ungeschoren aus einem solchen Fall hervorzugehen. Der Beamte selbst hat aber in der Folge eine solche Fülle von Scherereien, dass er schon sehr abgebrüht sein muss, um auf einen noch so wichtigen Festgenommenen zu schießen. Die Beamten haben einen Haufen von Vorgesetzten, die sich alle nach oben reinwaschen. Verfehlungen werden nach unten weitergegeben.

Sie kennen keine Kameradschaft, sondern nur Kumpanei. Jeder von ihnen will befördert werden. Jeder weiß, dass die Stellen begrenzt sind. Also konkurrieren sie. Sie wünschen dem Kollegen Niederlagen. Sie gönnen den Vorgesetzten den Anschiss von seinem Chef. Sie arbeiten unter Stress und wissen doch oder fühlen zumindest, dass eine Polizei mit ihrem Apparat noch lange keine Gewähr gegen eine nationale Revolution bietet.

Das soll natürlich nicht heißen, dass du nun „Verständnis“ oder gar Mitleid für die Lage der Polizeibeamten haben oder dich gar aufgrund einer gemeinsamen „Gesellschaftssituation“ mit ihnen verbrüdern sollst.

Das soll dir nur zeigen, dass die Polizeibeamten von Erfolgszwang und Existenzängsten getrieben sind und daß du in der Konfrontation keineswegs der Schwächere bist. Das wollen sie dir nur glauben machen. Deshalb müssen sie ihre Stärke mimen. Sie wollen dich kleinkriegen. Solange du nicht klein bist, sind sie es, in den Augen ihrer Vorgesetzten und in ihren eigenen.

11.4.9 Erkennungsdienstliche Maßnahmen

Erkennungsdienstliche Maßnahmen (Fingerabdrücke, Lichtbilder, Speichelprobe und ähnliches z.B. „Ganzkörpernacktaufnahme“) dürfen nach §81b StPO nur gegen Beschuldigte, nicht gegen Zeugen getroffen werden.

Sie müssen für die Ermittlungen notwendig und zu den vermuteten Straftaten verhältnismäßig sein.

Verlange, sofort deinen Anwalt telefonisch sprechen zu können.
Lege gegen die erkennungsdienstliche Behandlung sofort Widerspruch ein und beantrage die sofortige Aussetzung des Vollzugs.

Verlange (notfalls gerichtlich) die unverzügliche Vernichtung der erkennungsdienstlichen Unterlagen, wenn sie für die Ermittlungen nicht notwendig und zu den vermuteten Straftaten unverhältnismäßig sind. Dies kann gleichzeitig mit der Dienstaufsichtsbeschwerde gegen den/die handelnden Beamten geschehen (zu richten an die vorgesetzte Behörde, z.B. das Polizeipräsidium).

11.4.10 Die Einschüchterungstaktiken

Die Strategie, dich kleinzukriegen, setzt bereits beim ersten Zugriff der Polizei oder sonstigen Ermittlungsbehörden ein. Es treffen hier oftmals verschiedene Interessen zusammen: Sadistisch-erotische Neigungen der einzelnen Beamten, politische Interessen, der Wunsch, den Kollegen zu imponieren und schließlich das konkrete Ermittlungsinteresse.

Du wirst also bereits von Anfang an auf verschiedenen Ebenen in die Zange genommen, ohne dich in angemessener Weise wehren zu können. Sie schüchtern dich mit ihrem Aufwand an Waffen und Beamten ein. Sie versuchen dir mit Hilfe von besonderen Polizeigriffen Schmerzen zuzufügen. Sie drehen dir die Arme bis „zum Anschlag“ um, so dass du fürchtest, sie werden sie dir brechen. Anschließend wirst du in ein Polizeiauto geworfen. Dort erwarten dich dann Beamte, die dich mit Redensarten eindecken. Diese Redensarten sollen dir zeigen, dass du völlig in ihrer Gewalt bist. Du weißt, dass du später keinen für irgend etwas zur Verantwortung ziehen kannst, denn falls

du Anzeige erstattest, hat keiner der Beamten etwas gehört oder gesehen. Vor allem, wenn du eine Frau oder ein Mädchen bist, lassen sie ihren Reden und Phantasien oftmals freien Lauf. Sie diskutieren in deiner Gegenwart eingehend dein Äußeres, deine Fehler und Vorzüge. Sie bedrängen dich hart mit ihren Worten und Redensarten.

Wenn du ein Junge oder ein Mann bist, werden sie vor deinen Ohren das ganze Arsenal von Gewalttätigkeiten abspulen, dessen ihre Phantasie und wohl auch ihr Praxis fähig ist.

11.4.11 Erfahrungsbericht: Allein auf dem Revier

Auf dem Revier haben sie mir wieder die Handschellen abgenommen. Ich musste meine Taschen ausleeren und meine Personalien angeben. Dann kann ich wieder warten.

Die Festnahme geht mir wie ein Film durch den Kopf. Der Polizeiwagen, der plötzlich hinter mir ist. Dann noch einer, der mich überholt und sich querstellt. Sie springen mit gezogenen Pistolen heraus und zerren mich aus dem Auto. Eine Antwort auf die Frage, was das ganze denn soll, kriege ich nicht. Sie haben hier die Macht, und nur sie haben das Recht, Fragen zu stellen. Sie sind aufgeregt und warten nur darauf, dass ich irgend etwas sage oder wütend werde, damit sie mich verprügeln können. Ganz schön kaputt diese Typen.

Dann in Handschellen aufs Revier. Und nun sitz ich hier.

Erst haben sie mich behandelt wie einen Hochexplosivstoff und nun tun sie so, als wäre ich gar nicht da. Sie gehen raus und rein, telefonieren, reichen sich Akten zu und flüstern, man hat das Gefühl, dass sie dir ein ganz dickes Ding anhängen wollen. Und dann diese Warterei und Ungewissheit. Warum haben sie dir die Wohnungsschlüssel abgenommen? Du sitzt, wartest und machst dir immer verrücktere Gedanken.

Endlich kommt einer und führt dich in einen anderen Raum. Er fragt nochmals nach meinen Personalien und will dann wissen, wo ich vorher gewesen bin. In diesem Moment bin ich fast so weit, dass ich meinen Vorsatz, nur vor dem Richter auszusagen, aufgebe. Nur um hier schnell wegzukommen. Und das ist ja wirklich eine Kleinigkeit zu sagen, wo ich gewesen bin. Aber dabei wird es natürlich nicht bleiben. Die nächsten Fragen wären: „Wo waren sie vorher, mit wem und wen kennen Sie da.“

Also will ich doch erst einmal wissen, was mir vorgeworfen wird. Ich verlange meinen Anwalt zu sprechen. Nun muss ich wieder warten. Am besten, ich schlafe ein bisschen.

Schlimmstenfalls kriege ich einen Haftbefehl, dann werde ich eben das Gefängnis mal von innen kennenlernen. Schließlich hat die Warterei ein Ende.

„Kommen Sie mit“, sagt einer und einen Moment lang hoffe ich, nach Hause gehen zu können. Draußen wartet aber schon ein Wagen und ich muss einsteigen. Wohin es geht wird mir nicht gesagt. Die Sitzzelle im Auto ist wirklich winzig, keine Luft und eine Fahrt ins Ungewisse. Man wird hin und her geschaukelt. Das Auto hält und die Minizelle wird aufgeschlossen. Ich bin auf einer ganz normalen Straße.

Ein Schild: Gerichtsmedizinisches Institut.

Mir wird Blut abgezapft. Dann wieder ins Auto. Diesmal dauert die Fahrt etwas länger: Ein Krankenhaus, in dem eine Urinuntersuchung vorgenommen wird. Die Tür zur Toilette bleibt offen, damit ich nicht entwischen kann. Dann ist auch das überstanden und ich komme zur Gothaer Straße - Polizeigefängnis - und wieder warten.

11.4.12 Wovor haben die Polizeibeamten und die Herrschenden Angst ?

Das System, das diesen Apparat gegen dich mobilisiert, hat doppelte Angst. Sie wissen, dass ihre Tage gezählt sind, wenn du zu stark wirst. Ihre Stärke basiert auf Gewalt und auf der Demonstration von Gewalt. Dadurch wollen sie ihre Angst vor dir und deiner Idee verringern.

Dazu kommt die Angst derjenigen, die Helfer der Herrschenden sind: Die Beamten. Du wirst sie auch in Verhören immer wieder beobachten können. Sie wollen das treffen und vernichten, was sie für deinen Stolz halten. Es gehört zu den traditionellen Praktiken der Verfolgungsorgane, zunächst zu versuchen, den Festgenommenen oder Gefangenen in seiner Persönlichkeit, seinem Stolz und seiner Menschenwürde zu vernichten. Er soll in eine Situation gebracht werden, in der er sich selbst nicht mehr achten kann. Er soll weinen, schreien oder um Gnade bitten. Er soll einen Begriff von totaler Macht - und Hoffnungslosigkeit bekommen. **Du musst dich darin üben, deinen Stolz auf eine andere Grundlage zu stellen.**

Überlege dir genau, woran es liegt, dass dich Beamte, deren Funktion du rational genau einschätzen kannst, überhaupt beleidigen können. Du weißt, dass es eigentlich überhaupt keine Bedeutung für dich haben kann, was ein Polizist in einer solchen Situation zu dir sagt. Tatsächlich sind in uns aber eine ganze Reihe von Denk- und Verhaltensweisen lebendig, die sich nicht vom Verstand her wie durch einen Knopfdruck abschalten lassen.

Im Lauf der letzten Jahre hat es sich gezeigt, dass gerade diejenigen Leute am wenigsten gegen derartige Angriffe gewappnet waren, die meinten, ihre akademische „Überlegenheit“ von Bildung und Herkunft, ihr politisches Bewusstsein und die Freizügigkeit ihrer Lebensweisen machten sie dagegen immun. Diese Leute haben lernen müssen, dass in den Festnahmesituationen gerade diese „Überlegenheit“ nicht zählt, sondern völlig unwirksam ist.

11.4.13 Deine Schwäche ist Deine Stärke

Du musst dir die Zweigleisigkeit dieser Situation bewusst machen. Du bist auf der eben geschilderten Ebene der Schwächere. Die Polizei ist in der Überzahl und in einer Gruppe, in der sie sich nach außen sicher fühlt. Dennoch muss etwas an dir sein, was sie zu Äußerungen reizt, mit deren Hilfe sie sich selber bestätigen müssen. Wenn du tatsächlich das „Würstchen“ wärest, verlören sie kein Wort über dich. Sie würden sich mit dir dann bestimmt nicht auseinandersetzen.

Aber du reizt sie. Sie wissen oder spüren, dass ihre Überlegenheit nur so lange vorhält, wie sie dich im Wagen oder in der Zelle haben.

Du repräsentierst für sie eine Kraft, die sie politisch fürchten. Du repräsentierst ihre Zweifel an diesem System, ihre eigene Unterworfenheit, die sie ständig verdrängen und durch Kraftmeierei zu überspielen suchen. Du demonstrierst allein durch dein Dasein und deine Praxis Stärke, die ihnen ihre eigene Schwäche bewusst werden lässt. Diese Schwäche können sie nicht ertragen.

Deshalb demonstrieren sie Stärke, wie jemand, der seine Angst durch lautes Pfeifen verdecken will. Die Verhaltensforschung nennt das bei Tieren Imponiergehabe. Imponiergehabe hat nur der Schwächere nötig. Also steige nicht auf diese Ebene der Konfrontation ein. Du bist nicht der Schwächere. Du bist der Stärkere, den sie erst kleinkriegen wollen

11.4.14 Die Vernehmungstaktiken

Nach erfolgter Festnahme - im Gefangenentransportwagen, in der Polizeizelle bei der Kripo - setzen irgendwann die Versuche ein, Aussagen zur Sache aus dir herauszuquetschen.

Du kennst bereits die beiden Wege: den formellen, über eine Aussage, zu der du dich erst bereit erklären musst, und den informellen, über ein Gespräch bei einer Tasse Kaffee, im Gang oder von „Mensch zu Mensch“.

Die Informationen, die Beamte benötigen, haben zweierlei Charakter:

- Sie sollen in einem Strafverfahren verwendet werden, müssen also gerichtsverwertbar sein, d.h. sie dürfen nicht unter Umgehung von Gesetzen, z.B. dem § 136 StPO, zustande kommen.
- Sie sollen der weiteren Ermittlungsarbeit dienen. Hier darf die Ermittlungsbehörde jeden Hinweis verwerten. Hier wird zum Beispiel das Telefon eines Arztes abgehört, nur darf ein sich daraus ergebener Hinweis nicht im Verfahren verwertet werden.
- Wird aber aufgrund dieser widerrechtlich erlangten Informationen eine Hausdurchsuchung durchgeführt, so ist das hierdurch sichergestellte Material verwertbar.

Willst du also deine Rechte voll wahren, musst du sorgfältig darauf achten, dass Informationen, die du im Kopf hast, auf keinem Wege denselben verlassen. Das Gesetz geht von der Fiktion aus, der Mensch habe einen freien Willen, den er nach Belieben betätigen könne, auch der Entschluss gemäß § 136 auszusagen, sei frei, wenn er nicht unter den besonderen Umständen des § 136 StPO zustande gekommen ist.

Die Beamten werden dir also zunächst die gesetzlich zulässige „Entscheidungshilfe“ geben wollen. Dazu werden sie aus ihrer Maske als Kriminalbeamte heraus schlüpfen und versuchen, dir gegenüber die Rolle „Deines Anwaltes“ zu spielen. Anstatt dir sofort Gelegenheit zu geben, wirklich deinen Anwalt zu befragen, haben sie ein Interesse daran, diesen zunächst fern von dir zu halten.

Sie werden alle Register ziehen, um deinen freien Willen in ihre Richtung zu lenken.

11.4.15 Die Taktik des „Es ist das beste für Dich“

Sie werden versuchen, dir weiszumachen, das Beste für dich sei, auszusagen. Das geschieht, indem man dir vorhält, welche Strafen einen erwarten. Sie werden dir weiszumachen versuchen, deine Position sei ohnehin aussichtslos. Der Geständige aber erhalte Straferlass und komme möglicherweise nicht in die Untersuchungshaft, weil dann keine Verdunklungsgefahr bestehe.

Wenn sie Recht hätten, bräuchten sie die Zuziehung eines Anwaltes nicht zu fürchten. Es muss dich misstrauisch machen, dass sie dir raten wollen, es aber nicht zulassen, dass dies eine Person deines Vertrauens tut.

Nochmal:
Die Vernehmung ist nicht nur ein Spiel von Fragen und Antworten, sondern eine Situation, zu der nicht nur der Beamte und Befragte gehört, sondern ebenso deine Angst, seine Routine, die Wahl des Zimmers, die Beamten, die scheinbar nicht beteiligt sind, Hektik, Ungeduld und gespielte Szenen.

Der Beamte wird zunächst versuchen, mit dir ins Gespräch zu kommen. Man wird dir Ërmittlungsergebnissevorlesen, die dir zeigen sollen, wie weit man mit den Ermittlungen ist. Du kannst aber gar nicht beurteilen, ob dies tatsächlich Ergebnisse oder nur Vermutungen sind. Es ist vorgekommen, dass dem Beschuldigten Papiere als „Geständnisse“ vermeintlicher Mitbeschuldigter vorgelegt wurden, an denen kein Buchstabe echt war. Abgesehen davon, ist auch ein wirkliches Geständnis noch lange kein Grund, auf sein Schweigerecht zu verzichten, denn nur ein Anwalt kann beurteilen, ob dieses vermeintliche Geständnis echt ist. Weiter wird man versuchen, dich mit Namen, Adressen, Telefonnummern und Tatsachen aus deinem Leben, von denen du meinst, sie

seien unbekannt, zu überrumpeln.

Durchschaue diese Manöver. Wenn sie alles wissen, wozu dann noch eine Aussage. Wenn du bereits überführt wärest, wie wollen sie dir dann eine milde Strafe versprechen? Darüber entscheidet ohnehin das Gericht, das dir gewiss nicht dankbar ist. Wenn sie in der Rolle deines Anwaltes keinen Erfolg haben oder wenn sie merken, dass du dir von ihnen nichts einreden lässt, werden sie versuchen, dich psychisch zu bearbeiten.

11.4.16 Gespräche von „Mensch zu Mensch“

Bereits im Transportwagen in der Polizeizelle oder bei der Kripo, wenn es dir bereits besonders dreckig geht, wird ein Beamter in der Rolle des „Freund und Helfer“ auf dich zukommen. Das kann ein „Höherersein“, der die Polizisten, die dich beschimpfen, zur „Ordnung“ ruft. In deiner miesen Situation neigst du dazu, dich an diesen Strohhalm zu klammern und zu vergessen, dass er derjenige ist, der jetzt den Auftrag hat mit dir in ein vertrauensvolles Gespräch zu kommen. Es passiert nicht selten, dass gerade dieser Beamte sich später vor Gericht rühmt, er habe es eben mit seiner verständnisvollen Art geschafft, das Vertrauen des Beschuldigten zu erlangen, der ihm schließlich das Herz ausschüttete. Die Taktik besteht darin, dich zunächst in eine Situation zu bringen, in der es dir schlecht geht, damit dann einer als dein „Freund und Retter“ auftreten kann. Oft werden zu diesem Zweck auch Vernehmungen mit verteilten Rollen durchgeführt:

Einer ist scheinbar der Sachliche, der die Vernehmung offiziell vornehmen soll.
Zwei weitere Beamte sind im Raum entweder als Zuhörer oder scheinbar mit etwas Anderem beschäftigt.

Du verweigerst die Aussage. Dein sachliches Gegenüber versucht dir in Güte zuzureden. Du schweigst. Er brüllt los: „Mit euch müsste man kurzen Prozess machen...“ Dabei kommt er dir so nahe, dass seine Nase dich fast berührt. Du riechst seinen Atem und bekommst seine Spucke ins Gesicht. Er brüllt weiter, bis nun dem Dritten die Sache „zuviel“ wird. Er schickt den Schreier raus und befreit dich von ihm. Er wird dir sagen, dass sie den auch nicht leiden können, dass er bald versetzt wird. Dann bieten sie dir eine Tasse Kaffee an. Du empfindest Dankbarkeit. Du solltest Dankbarkeit empfinden.

Die Beamten wissen, dass wir in bestimmten Situationen nach Mustern und Mechanismen zu reagieren pflegen. Wir sind einfach darauf gestimmt, jemandem, der uns hilft, dankbar zu sein oder dem, der uns Verständnis entgegenbringt, freundlich zu begegnen. Das muss im normalen täglichen Umgang auch nicht falsch sein. Aber diese eingeschliffenen Mechanismen des täglichen Lebens sind uns so in Fleisch und Blut übergegangen, dass sie auch in Situationen aktiv sind, wo sie überhaupt nicht angebracht sind. Das Verhältnis zwischen Beamten und Beschuldigten ist in keiner Situation geeignet, Freundlichkeit oder Dankbarkeit aufkommen zu lassen. Auch wenn es dir schwer fällt, mit dem Beamten, dem du „Dank schuldest“, nicht zu sprechen, in ihm immer noch den Systemschergen zu sehen. Vergiss nicht, dass es dein Recht ist, zu schweigen. Wenn der Beamte erst seine Macht darauf verwendet, dich unter Druck zu setzen und dann den Druck lockert, ist es absurd, hierfür auch noch dankbar zu sein. Selbst wenn er den Kaffee aus eigener Tasche bezahlt, ist das eine Investition, die sich für ihn spätestens bei der nächsten Beförderung auszahlt.

Diese „Retter“ sind die gefährlichsten Personen in diesem abgekarteten Spiel. Sie wollen deinen Kopf, deine Aussage und deinen Entschluss zum Geständnis. Du hast zu kämpfen, um ihnen zu widerstehen. Und wenn du meinst, deine Dankbarkeit wirklich nicht verkneifen zu können, kannst du dem Beamten später, wenn du aus der Sache raus bist, immer noch eine Büchse Bier als Dank schicken. Aber keine Aussage! Wenn der Beamte seine mmenschlicheSeite zeigt, verweigere nicht nur jede Aussage, sondern lass dich auf kein Gespräch von „Mensch zu Mensch“ ein. Er wird dir erzählen, dass er auch Kinder hat, die womöglich „rechts“ eingestellt sind. Er findet vieles ja auch

richtig und versteht auch die Jugend; er würde ja auch mitmachen. Er wird versuchen, dich in eine Diskussion zu verwickeln, innerhalb der er dich langsam auf eine Bahn bringen kann, die dann zu einer Aussage Führt. Außerdem verstärkt sich deine emotionale Beziehung zu ihm. Du findest ihn freundlich und fühlst dich verstanden. Das hat zur Folge, dass du bewusst oder unbewusst dich selbst veranlasst fühlst, freundlich zu ihm zu sein und ihn zu verstehen. Du beginnst jetzt Angst zu haben, ihn durch weiteres Verweigern zu „enttäuschen“.

Der Leim ist süß, auf dem du kriechen sollst.

11.4.17 Erfahrungsbericht: Die Vernehmung

Äls sie mich am nächsten Tag zur Vernehmung holen, bin ich froh, aus meiner Zelle herauszukommen. Ich bin froh, Menschen zu sehen, freundliche Gesichter, und als sie mir eine Zigarette anbieten, rutscht mir ganz automatisch ein „Danke“ von den Lippen. Da ist ein helles Bürozimmer, Blumentöpfe, eine Sekretärin kocht Kaffee und schon bist du eingestimmt auf ein normales - „Mensch zu Mensch“ Verhalten. Du willst niemanden vor den Kopf stoßen. Es fällt mir schwer, auf ihre freundlichen Fragen nicht zu antworten, und ich hatte mir die Polizisten ganz anders vorgestellt. Der eine ist jung und hat kurze Haare; der andere ist graumeliert, braungebrannt und ganz väterlich. Sie wollen nichts weiter als sich mit dir ein bisschen unterhalten.

Ohne Protokoll und Tonband sagen sie; sie wollen nur wissen, was wir so denken. „Es muss ja was dran sein, wenn man sich jahrelang für eine Sache einsperren lässt.“ Sie sind ja auch nicht mit allem zufrieden, die vielen Ausländer, die Umweltzerstörung, da müssten wir doch mal was machen. Und dann gibts ja heute so viele Gruppen und Parteien, da findet sich ja kein Mensch mehr zurecht. Der Ältere war noch in der HJ und er hat gute Erinnerungen daran. Damals war noch Disziplin in Deutschland. Der Jüngere sagt, dass damals noch etwas galt und nicht Chaoten wie in der Hafenstraße von den Politikern und der Presse gehätschelt wurden.

Ganz unscheinbar sind sie zu zwei Bürgern geworden, die nur zufällig im Beruf Polizist sind. Sie wollen sich gerne überzeugen lassen, nur hat es ihnen bisher noch nie jemand so richtig erklärt. Vielleicht denkst du, sie sind ja auch vom Geld abhängig und ausgebeutet; wer weiß, wie viele da schon Dinge sagten, die sie gar nicht sagen wollten.

Als ich immer noch nichts sage, wie ein Klotz dasitze und aus dem Fenster starre, versuchen sie, an mein Ehrgefühl und an meine Aufrichtigkeit zu appellieren. Wenn ich etwas getan hätte, müsste ich doch dazu stehen Ëin Deutscher steht zu seiner Tat.Ës handele sich ja um nichts Kriminelles, sondern um was Politisches. Wie wolle man ein Beispiel geben, wenn man nicht zu seiner Tat stehe? Das würden sie respektieren, da hätte ja manch Krimineller mehr Ehrgefühl im Leibe. „Machen sie reinen Tisch. Sie wissen, die Gerichte werden es Ihnen zu Gute halten“.So wären sie leider gezwungen, deinen ganzen Bekannten- und Freundeskreis zu überprüfen, die würdest du nun auch noch mit in die Sache reinziehen. Und immer offener und drohender werden sie, sie hätten eh schon genug Material, das reiche schon für ein paar Jährchen. Man könne dich hier in einer Ecke verschimmeln lassen, mit solchen wie dir werden sie schon lange fertig, und nicht alle Beamten wären so freundlich wie sie. Der „Väterliche“ schlägt plötzlich mit der Faust auf den Tisch und schreit, er habe jetzt genug von dir. Dann bringen sie mich nach unten in einen Gitterverschlag und lassen mich ein paar Stunden ßchimmeln.Diese Stunden wollen kein Ende nehmen. Du willst dösen, kannst nicht, hin- und hergehen geht auch nicht. Und ständig gehen dir Fragen durch den Kopf. Worauf wollen sie heraus? Was haben sie mit mir vor? Schließlich kommen sie wieder. „Na, haben Sie sich es überlegt, wollen Sie jetzt unsere Fragen beantworten? Ich will noch nicht: Aber jetzt haben auch sie genug. Sie lassen mich in Ruhe, und ich werde zurück ins Untersuchungsgefängnis gebracht. Diesmal erscheint mir meine Zelle fast wie ein Paradiesv

Ein Weiteres Beispiel für die Taktik der Polizeibeamten: Sie versuchen, die Beziehung zu Personen, die uns emotional nahe stehen, auszunutzen.

Wenn sie anders nicht mehr weiterkommen, greifen die Beamten zu dem Mittel, den zu Vernehmenden mit seinen Eltern, seinen Freunden, seinen Ehepartner, seinen Kindern oder anderen Personen zusammenzubringen. Sie gehen davon aus, dass es in unserer Verwandtschaft oder unter den Menschen, denen wir uns verbunden fühlen, jemanden gibt, der in der Lage ist, uns umzustimmen. Die Spekulation der Beamten ist folgende: Sie sehen, Zwang und Drohung, Überredung und Verängstigung helfen nicht. Sie haben auch keine Beamten, die in der Lage sind, zu dir eine emotionale Beziehung aufzubauen, so dass du dem Beamten zuliebe aussagen würdest. Also wählen sie unter Bezugspersonen Leute aus, denen zuliebe du einiges tun würdest, die du nicht enttäuschen willst, denen gegenüber du Anlass zu Respekt oder Dankbarkeit hast. Es müssen Personen sein, die politisch und juristisch nicht durchblicken, also nicht durchschauen, wofür sie benutzt werden sollen. Sie sollen die Doppelrolle des Lockvogels spielen:

Einerseits Deinesgleichen, mit dir befreundet oder verwandt, andererseits im Dienst derer, die dich kleinkriegen wollen. Und sie merken es nicht, weil sie oft einem anderen Denken und Wissen verhaftet sind. Die Frage, ob du aussagst oder nicht, soll zu einer Entscheidung zwischen dir und deinen Eltern, zur Existenzfrage deiner Beziehung zu ihnen hochgeschraubt werden.

Es gehört zu den größten Zynismen der Polizei, die Eltern eines Betroffenen zu benutzen, um ihn in die Knie zu zwingen. Jeder weiß, dass gerade die Eltern den Angstmechanismen noch viel mehr unterworfen sind als wir, die wenigsten einen relativ größeren Durchblick haben. Eure Eltern haben den Beamten gegenüber häufig überhaupt keine Widerstandskraft. Sie scheuen sich noch mehr als ihr dem freundlichen Beamten „unfreundlich“, also angemessen zu begegnen. Sie sind in ihrem Zweifel oft schnell genug bereit einzusehen, dass es für ihr Kind doch nicht gut sei, sich weiterhin zu weigern. Sie sind meist die geeignetsten Opfer für alle Drohungen und Schwarzmalerei der Beamten. Dann kommen sie zu dir in die Zelle. Es geht dir nicht gut. Sie sehen das und du siehst sie weinen, leiden und dich beschwören. Und du sagst kein Wort. Aber du hast Angst, sie ganz kaputt weggehen zu sehen. Du weißt nicht, wie du ihnen deine Lage begreiflich machen sollst. Du entwickelst Ihnen gegenüber Schuldgefühle. In dieser Situation darfst du nicht vergessen, dass deine Schuldgefühle die genau einkalkulierte fünfte Kolonne der Beamten sind. Die Schuldgefühle sollen in dir die Arbeit der Beamten leisten und dich zum Fallen bringen. Diese Situation gegenüber deiner Frau, deinem Mann oder Kindern ist noch viel schlimmer, weil sie zu der emotionalen Seite noch deine Verantwortung hinzufügen. Zu ihnen darfst du ein Wort sagen: Sie sollen mit deinem Anwalt sprechen; der kann ihnen dann erklären, wie deine Situation aussieht. Aber nur mit deinem Anwalt. Verzichte auf jede Rechtfertigung und Diskussion

Eine weitere Schwäche, auf die Beamten zählen, ist unsere Neigung, unser Tun überall und gegenüber jedem zu rechtfertigen. Vielen von uns ist es unerträglich, mit dem Gedanken herumzulaufen, etwas zu tun, dieses aber nicht zu rechtfertigen. Auch das mag in manchen Situationen des täglichen Lebens richtig sein. In der Situation der Vernehmung ist es absolut falsch. Es ist genauso falsch, auf die Idee zu kommen, den Beamten gegenüber jetzt zwar keine Aussage zu machen, ihnen aber haarklein darzulegen, dass man nur seine Rechte als Beschuldigter wahrnimmt.

Denk daran:
Kein Wort der Rechtfertigung. Überlege dir lieber, wer Anspruch auf Rechtfertigung hat: Nur wer dich auch kritisieren darf. Du wirst zugeben müssen, dass der Beamte hierzu nicht die Berechtigung hat. Auf irgendeine Art wird der Beamte immer wieder versuchen, mit dir ins Gespräch zu kommen. Er wird dich zum Beispiel bei deiner Intelligenz packen wollen, oder er wird versuchen, mit dir politisch zu diskutieren. Hierbei benutzt er Wissen, welches er sich im Laufe seiner Arbeit aneignen musste. Er hat sich sicher mit einigen politischen Schriften beschäftigt. Er wird versuchen, bei dir die Stellen herauszufinden, in denen du möglicherweise unsicher bist, in denen du politisch vielleicht verzweifelst. Er wird mit allen möglichen Zitaten aufwarten, um dir zu erklären, dass „Ihr“ politisch falsch liegt. Vielleicht trifft er genau die Position, die du selbst in Diskussionen mit deinen Kameraden erfolglos vertreten hast. (Er kennt sie vielleicht aus V-Material). Du

meinst, bei ihm „echtes“ Interesse zu spüren. **Lass ihn sich abzappeln! Er hat mit dir nichts zu tun. Er macht die Sprünge schließlich nur, um dich zum Reden zu bringen. Wenn er wirklich politisches Interesse hätte, bräuchte er nicht warten, bis du antwortest.**

Du hast es nicht nötig, den Beamten zu imponieren. Hüte dich davor, deinem Gegenüber in dieser Situation in irgendeiner Weise zu imponieren. Frag dich lieber, ob es nicht zu ertragen ist, längere Zeit mit einem Beamten zusammenzusein, ohne es ihm wenigstens einmal „zu geben“. Denk daran, dass deine Position nicht nur schwach, sondern auch stark ist. Mach nicht den Fehler, dem Anderen zeigen zu wollen, dass du der Stärkere, der Klügere, der Gebildetere und politisch Bewusstere bist; denn dann bist du der Dumme. Er wird sofort darauf einsteigen und dir mit Interesse folgen und durch „dumme“ Zwischenfragen deinen Redefluss ankurbeln. In Wirklichkeit kannst du ihm nur dadurch imponieren, dass du in jeder Situation bei deinem Schweigen bleibst.

11.4.18 Die Taktik des „Sie haben gewonnen“

Eine weitere Gefahrenquelle ist die Euphorie, die sich einstellt, wenn man meint:

Ich habe es geschafft. Fast jeder weiß, wie man sich fühlt, wenn man aus einer Drucksituation befreit wird. Man ist gesprächig, fröhlich und redet wie aufgedreht, z.B. wenn man eine Klassenarbeit, eine Klausur oder eine Prüfung erfolgreich hinter sich hat. Man fühlt sich unbeschwert, wenn man die Last los ist. In dieser Stimmung hat man wenig Lust, noch weiter an die Strapazen zu denken. Man vergisst schnell die Mühsal und damit leider auch jede Vorsicht.

Nach einer langwierigen Druckperiode in einem Vernehmungszimmer, nach allen möglichen Beschimpfungen, Anfeindungen und all den Strapazen wird plötzlich gesagt: Schluss, es hat keinen Zweck, er will nicht, gut. „Sie haben gewonnen.“, sagt ein Beamter zu dir. Du bist froh, stolz und weißt, dass du gut warst. Warst du auch.

Aber Schluss ist eben nicht dann, wenn sie es sagen. Jetzt beginnt ein neuer Rollenwechsel. Du siehst die Beamten, mit denen du zu tun hattest, erschöpft. Sie waren erfolglos. Sie übergeben dich jetzt einen anderen, den du noch nicht kennst. Der hat nur den Auftrag, mit dir etwas zu essen, oder dich ins Gefängnis zurückzubringen. Er scheint völlig unverdächtig. Er fragt dich, ob du sie fertiggemacht hast. Er spielt Schadenfreude. Du freust dich, dass du jemanden hast, der deine Freude teilt - aber auch er wartet nur auf deine Worte.

11.4.19 Die Taktik, Kameraden gegeneinander auszuspielen

Fall nicht darauf rein, wenn man dich zusammen mit anderen Gefangenen oder sogar mit Kameraden transportiert, warten lässt oder gemeinsam vernehmen will. Das ist nur ein weiterer Versuch, Aussagen von dir zu bekommen, auf die die Gegenseite schon lange wartet. In dieser Situation gibt es zwei Möglichkeiten:

- Du kennst den anderen (natürlich nicht richtig, sondern einigermaßen gut). Dann vermeide jede Geste des Wiedererkennens. Oft ist bereits so etwas Gegenstand von Ermittlungen. Fallt euch nicht um den Hals. Fragt nicht nach dem Tun der letzten Zeit. Sprecht nicht von früher. Sprecht auch nicht, wenn ihr alleine seid über Dinge, die die Polizeibeamten mithören könnten. Wenn er Durchblick hat, begreift er es. Wenn nicht, ist es um so gefährlicher.
- Auch hier gilt es, dass es besser ist, jemanden vor den Kopf zu stoßen und es später mal zu erklären, als sich und andere um seine Rechte und in Gefahr zu bringen.
- Du kennst den Anderen nicht. Dann sprich nicht über dich, sondern nur über ihn. Gib keine Kommentare. Sprich über das Wetter, den Knast, Essen und Sport. Auf keinen Fall über deinen Fall. Vermeide auch hier Imponiergehabe. Hab den Mut, für ein Würstchen gehalten

zu werden. Wenn du wieder draußen bist, werden sie wissen, dass du keines warst. Denk daran, dass sie auch Pannen spielen können. Es ist durchaus möglich, dass sie dich „versehentlich“ mit jemanden zusammentun, von dem sie dich vorher streng isoliert haben. Deine Freude musst du dann zügeln. Verhalte dich so, dass sie aus deinem Verhalten keinerlei Informationen ziehen können. Was für Begegnungen mit Personen gilt, trifft auch auf Orte oder Sachen zu. Nicht selten wird ein Betroffener an Orte gefahren, von denen angenommen wird, dass er sie kennt. Die Polizeibeamten wollen an der Reaktion prüfen, ob sie mit bestimmten Vermutungen auf dem richtigen Weg sind. Richte dein Verhalten danach ein. Werde nicht plötzlich in einer bekannten Gegend munter und recke den Hals, wenn du vorher geschlafen hast. Gib keine Hinweise auf Ort - oder Wegkenntnisse.

Wenn man dir Sachen, wie Waffen, Kleidung, Schlüssel, Autos oder sonst etwas zeigt, zeige für nichts davon Interesse. Nimm auch nichts davon in die Hand. Man kann aus der Art, wie jemand etwas anfasst, sehr gut sehen, ob er gewohnt ist, damit umzugehen

11.4.20 Wie bekommst Du Kontakt zur Außenwelt ?

Einer der Hauptquellen deiner Angst ist die Abschottung. Du hast keine Ahnung, wann Hilfe kommt und weißt nicht, wie lange die Prozedur dauert. Es gehört zu den Praktiken der Polizei, dir zunächst nicht zu sagen, wann du entlassen wirst. Sie lassen dich in dem glauben, dass du verhaftet werden sollst und dass du mindestens 14 Tage drinnen bleibst. Auch wenn sie dich noch am gleichen Tag entlassen. Wir wissen auch, dass man wegen einer Lappalie oder ohne, dass man etwas strafbares getan hat, verhaftet werden kann.

In dieser Situation heißt es Ruhe bewahren und sich auf den schlimmsten Fall einzustellen. Der schlimmste Fall ist zunächst die Vorführung vor einem Richter. Das muss in der BRD spätestens vor Auslauf des auf die Festnahme folgenden Tages geschehen. Obwohl eigentlich die Vorführung vor einen Richter unverzüglich zu erfolgen hat, nutzt die Polizei diese Frist voll aus. Du musst dich auf diese Frist einstellen.

Diese Zeit musst du nutzen. Schlafe und entspanne dich. Zwinge dich zum Abschalten. Denk darüber nach, was du deinen Anwalt sagen wirst. Lies, mach Denksportaufgaben oder sonst etwas, was dich ablenkt. Mach dich nicht fertig wegen möglicherweise gemachter Fehler.

Beobachte die Menschen in deiner Umgebung. Merke, was sie sprechen, wie sie heißen oder wie sie sich anreden. Achte genau auf ihr Äußeres und sag kein Wort. Wenn man dir Essen, Trinken oder eine Zigarette gibt, dann nimm sie und sag keinen Ton. Erst wenn sie dich zur Vernehmung holen, wenn du vor der Schreibmaschine sitzt, dann kannst du sagen, dass du einen Anwalt sprechen willst. Sag gleich welchen, damit sie nicht irgendeinen nehmen.
Jetzt gibt es zwei Möglichkeiten:

- Sie lassen dich mit einen Anwalt sprechen oder mit seinem Büro. Dann sag ihm deinen Namen, wo und unter welcher Begründung man dich festgenommen hat und wo du bist. Oft wird es so sein, dass der Anwalt im Moment nicht kommen kann. Dann sei nicht enttäuscht. In dieser Situation kann der dir ohnehin nicht helfen. Sie sind nicht einmal verpflichtet, ihn zu dir zu lassen. Dein Anruf hat aber den Wert, dass draußen jemand weiß, wo du bist. Er kann sich dann sofort um dich kümmern, wenn du verhaftet werden solltest.
- Wenn sie dich nicht mit ihm sprechen lassen oder wenn dein Anwalt in einer anderen Stadt wohnt, dann warte bis du dem Richter vorgeführt wirst.

Der Richter muss ein Protokoll aufnehmen, auch wenn du keine Aussage machst. In dieses Protokoll lass folgendes aufnehmen:
Ich beauftrage Rechtsanwalt xyz, Ort, Straße mit meiner Verteidigung. Ich beantrage für diesen

Anwalt:
einen Sprechschein
eine Abschrift dieses Haftbefehls (falls einer ergeht)
eine Abschrift dieses Vorführungsprotokolles zuzusenden.

Das hat zur Folge, dass der so benachrichtigte Anwalt dich schnell besuchen kann und dass er weiß, um welchen Sachverhalt es sich ungefähr handelt. Er kann aufgrund der in das Protokoll diktierten Vollmacht sich als dein Verteidiger legitimieren. Falls er verhindert ist, kann er gleich in die Wege leiten, dass dich ein anderer Anwalt besucht, zu dem du gleich Vertrauen haben kannst. Aber auch wenn der nicht gleich kommt, nachdem deine Post ihn erreicht haben müsste, gerate nicht in Panik. Manchmal lässt sich das nicht so schnell einrichten. Manchmal ist der Anwalt verhindert oder verreist. Dann schreib nochmals. Dränge ihn dir wenigstens schriftlich zu antworten. Das klappt meistens. Lass dich nicht von der Umgebung im Knast oder in der Polizeizelle fertig machen. Das alles ist geeignet, dich in Panik zu versetzen. Es stinkt und es ist kalt. Du hast Hunger und Durst. Neben dir schnarchen Betrunkene, andere stöhnen oder schreien. Im diesem Moment hilft nur: Abschalten, Schafen oder genaues Beobachten. Achte auf jedes Detail deiner Umgebung. Das lenkt dich ab, und es kann sich später als nützlich erwiesen. Versuche immer eine eiserne Reserve von Geld bei dir zu haben. Fünf Euro, um wenigstens nur zwei Tage Zigaretten zu haben. Zigaretten sind Knastwährung. Du kannst dafür Briefpapier, Bleistift und Briefmarken erhalten, die du nur an deinen Verteidiger brauchst.**Besser ist allerdings, du bist gar nicht erst von Zigaretten, Alkohol oder sonstigen Mitteln abhängig.**

Nutze die Wartezeit für Planungen: Was ist draußen zu regeln? Am Arbeitsplatz, in der Wohnung oder in der Schule? Müssen die Kinder versorgt werden? Welche Verwandten müssen beruhigt und welcher Chef muss benachrichtigt werden? Solche Sachen kannst du auch aufschreiben. Nur nichts, was mit deiner Verhaftung zu tun hat. Wenn du es nicht unbedingt aus psychischen Gründen zum Abreagieren von Wut nötig hast, leiste keinen Widerstand gegen Transporte, erkennungsdienstliche Maßnahmen oder sonstige Praktiken der Polizeibeamten. Du kannst dir sicher sein, dass sie stets in der Lage sind, diesen Widerstand gewaltsam und unter Schmerzen zu brechen. Für die Beamten ist das eine gute Gelegenheit, dir deine Unterlegenheit auf dieser Ebene zu demonstrieren und dich nicht nur psychisch, sondern auch körperlich zu schwächen. Es ist schlecht wenn du jetzt nicht nur wegen deiner Nervosität, sondern auch wegen der Schmerzen an Armen, Beinen, Rippen und Handgelenken nicht schlafen kannst

11.4.21 Untersuchungshaft

Wenn der Richter gegen dich einen Haftbefehl erlassen hat und du in das Untersuchungsgefängnis eingeliefert worden bist, findest du dich in einer völlig neuen Situation, in die du dich erst einmal reinfinden musst.

Um auch hier den verunsichernden, entnervenden Überraschungseffekt zu mindern, informiere dich bei ehemals inhaftierten Kameraden eingehend über das Leben im Knast. Über deine Rechte auf Einkauf, Verkehr mit der Außenwelt, Verhältnisse zu Wärtern und Mitgefangenen und Beschäftigungsmöglichkeiten im Knast. Abgesehen davon, dass es zum politischen Wissen von Kameraden gehören muss, die Unterdrückungsmittel des Staates auch in ihrer praktischen Anwendung und Wirkung zu erkennen, hilft es bei der Bewahrung deines Selbstbewusstseins.

11.4.22 Erfahrungsbericht: In der Zelle

„Sie führen dich einen Gang entlang, links eine Eisentür, rechts eine Wand, schließen eine Tür auf, gehen mit dir rein - so, da sind wir und dann gehen sie wieder raus und schließen die Tür hinter dir zu. Ein Tisch, ein Stuhl, ein Bett, ein Schrank, ein Waschbecken und ein Klo. Du stehst da und denkst nichts weiter als, „Ich will hier raus!“. Von draußen trennen dich drei verschlossene Eisentüren, die Wände sind dick, und das Fenster ist vergittert. Wie komme ich nun hier wieder

raus. Du steigst auf einen Stuhl, schaust dir das Gitter an und merkst, dass es fest sitzt. Nun schaust du in den Hof - Mauern, keine Menschenseele. Kein Mensch, mit dem du reden könntest, nur Feinde. Wärter und Aufpasser. Sie lauern hinter der Tür und beobachten dich durch den Spion. Sie herrschen dich an: du solltest von dem Stuhl herunterkommen, das sei verboten. Jetzt haben sie dich in ihrer Gewalt und das lassen sie dich spüren. Sie können kommen, wann sie wollen: Ob du beim Essen bist, beim Zähneputzen oder auf dem Klo. Wer weiß, was sie noch alles mit dir vorhaben. Du gehst auf und ab und gerätst langsam in Panik. Dir fallen von Leuten Geschichten ein, die verprügelt wurden, und von Leuten, die wahnsinnig wurden. Jedes Mal, wenn du draußen die Schlüssel scheppern hörst, zuckst du zusammen. Und dann die schreckliche Enge. Dauernd stößt du dich an irgendeiner Ecke vom Tisch, vom Waschbecken oder vom Bett.

Du kannst dich nicht bewegen, kannst nicht schnell mal in die Küche gehen und dir einen Kaffee machen oder schnell mal an die Ecke und dir eine Zeitung holen. Du hast nichts zu tun. Du sitzt und wartest."

Auch als Untersuchungsgefangener hast du in der BRD nach dem Wortlaut der Gesetze - Grundgesetze, Strafprozessordnung, Untersuchungshaftvollzugsordnung - eine Anzahl von Rechten.

Nach dem Gesetz dürfen diese nur insoweit eingeschränkt werden, wie es die Durchführung der U-Haft oder die SSicherheit und Ordnung der Anstalterfordern. Auch das ist Propaganda. In Wirklichkeit werden deine Rechte unter allen möglichen Vorwänden von den Gerichten, aber auch von der Anstaltsbürokratie ständig und auf verschiedenste weise eingeschränkt. Merke dir, Sicherheit und Ordnung gehen über alles. Zuerst kommt die Haftanstalt und dann erst der Gefangene.

Die Ordnung und Sicherheit der Anstalt wird unter anderem gefährdet durch:

Sprechen mit anderen Gefangenen
Annahme und Abgabe eines Päckchen Tabak
ein eigenes Radio (weil irgend jemand aufgebracht hat, man könne aus jedem UKW-Teil sofort und ohne Zusatz einen Sender bauen)
einen eigenen Fernseher (weil man mit der hohen Stromspannung die Wärter unter Strom setzen könnte)
zu viele Bücher oder Zeitungen in der Zelle (weil es dann unübersichtlich wäre)
eine Uhr (weil man dann die Flucht verabreden könne)
eigene Unterwäsche (weil man nur einem Flüchtling in Anwaltswäsche ansieht, dass er geflohen ist)
und nicht mehr als einmal vierzehntägig Besuch (weil sonst die Anstalt überlaufen würde)

Die Begründungen in den Klammern stammen von deutschen Gerichten oder Haftanstalten!

Dein Briefverkehr wird häufig auf zwei zweiseitige Briefe pro Woche eingeschränkt. Der Grund dafür ist meist, dass die Richter der Auffassung sind, es sei nicht ihre Aufgabe, den unbehinderten Kontakt des Gefangenen zur Außenwelt zu gewährleisten und durchzusetzen. Sie empfinden diese Pflicht als lästig und entledigen sich ihrer durch einen halbseitigen Beschluss.

Untersuchungshaft ist schlimm. In vielen Fällen bedeutet sie für den politischen Gefangenen ein staatlich legitimiertes Verbrechen an seiner Persönlichkeit, seiner seelischen und kärperlichen Gesundheit und der sozialen Existenz. Der Staat praktiziert seine Macht am Beispiel vieler Einzelner, damit das Volk Angst vor dieser Macht hat. Es soll die Unterdrückung draußen, immer noch der Qual drinnen vorziehen und nicht auf „dumme" Gedanken kommen. Wir wissen also: Der Zweck der Untersuchungshaft (Beugehaft) ist nicht nur der, der in den Gesetzen steht. Vielmehr soll jeder so starke Angst vor der totalen Unterdrückung seiner Persönlichkeit, seiner sozialen Kontakte und der Zerstörung seiner Existenz haben, dass er die Finger von allem lässt, was nach Knast riecht. Gleichzeitig soll ihm Wut und Lust vergehen, sich irgendwie den Anstaltszwängen zu widersetzen,

die ihm seine verbrieften Rechte nehmen. Auch hier ist unsere Angst der Verbündete der Gegenseite. Da man Angst nicht einfach abschalten kann, muss man Techniken entwickeln, ihrer Herr zu werden.

Vergewissere dich über deine Rechte und Möglichkeiten, sobald du im Knast angekommen bist.
Frage nach den Möglichkeiten, Zeitungen zu abonnieren und Bücher zu bestellen.
Häufig kann man dies nur an bestimmten Tagen in der Woche.
Es ist ärgerlich, aus Nachlässigkeit acht Tage auf Hilfe Anderer angewiesen zu sein, die oft selbst nicht viel haben.
Vergewissere dich, wie du an einen Arzt kommst oder an eine warme Decke.
Wie du Diätkost oder Zusatznahrung bekommst.
Sieh dir den Pfarrer oder Fürsorger an.
Du brauchst sie ja nicht gleich in dein Herz zu schließen, aber es ist gut zu wissen, wie sie aussehen.

11.4.23 Den Knast studieren

Verschaffe dir alle erreichbaren Kenntnisse über die Knastorganisation, die soziale und psychische Zusammensetzung und die Lage der Insassen und Beamten. Betrachte ihn als dein Studienprojekt, als wärst du auf einer Expedition.

Das ermöglicht dir, fundierte Kenntnisse über die Funktion und Wirkung eines der wichtigsten Herrschaftsinstrumente zu erwerben und hilft dir, dich selbst richtig zu verhalten. **Du wirst dabei auch lernen, welche Taktik andere Gefangene im Laufe ihres Lebens für ihr Überleben im Knast anwenden.**

Im Knast studieren
Lerne Dinge, die du bisher draußen nicht gelernt hast. Wenn dich Physik und Chemie nicht reizen können, so kannst du versuchen, Sprachen zu lernen.

Halte dich körperlich fit
Du hast pro Tag eine dreiviertel Stunde lang Bewegung im Ferien. Das hat zur Folge, dass du Fett ansetzt und dein Kreislauf schwach wird. Zwinge dich vier oder fünf Mal am Tag zu Übungen, die regelmäßig deinen Kreislauf und deine Muskulatur belasten. Du weißt noch vom Sportunterricht, was hierfür in Frage kommt: Liegestütz, Kniebeuge, Bauchmuskeltraining und Übung, für die Rückenmuskulatur. Bestell dir aus dem Buchhandel entsprechende Literatur.

Wenn du dich beschäftigen kannst, dann bekommst du auch nicht das Gefühl, die Zeit, in der du eingesperrt bist, sei verlorene Zeit. Sie ist es nicht. Wer drinnen ist, wird dir sagen, dass dort das Leben weitergeht. Zwar unter vielen Entbehrungen und Demütigungen, aber letztlich nicht so schlimm, wie alle, die draußen sind, es befürchten.

Dein Verhalten zu Mitgefangenen, wenn du mit ihnen in Berührung kommst, ist von zweierlei geprägt: Der gemeinsamen Situation im Knast und der unter Umständen vorhandenen, oft verborgenen Interessenlage zwischen dir und den Anderen. Das heißt: Trenne die Knastsolidarität von der politischen Solidarität

Der Knast ist in vieler Hinsicht ein Abbild der Gesellschaft draußen, mit allen Widersprüchen und Verhaltensweisen. Die Gemeinsamkeit der Situation als Gefangener bedingt, dass man sich gegenseitig die Entbehrungen und Unterdrückungen erträglich macht. Das geschieht durch Gespräche, Begegnungen und materielle Hilfe. Wer hat, gibt dem, der nichts hat. Man tauscht Zeitungen und Bücher. Man kann auch von seinem „Eigengeldkonto“ Geld auf das von anderen äberweisen oder seinen Anwalt auffordern, sich um einen Mithäftling zu kümmern. Diese allgemeine Hilfsbereitschaft darf aber nicht nach dem „Gießkannenprinzip“ praktiziert werden.

Auch im Knast gibt es typische Hierarchien - Reiche und Arme, Dealer und Zuhälter, die meist von draußen her über viel Geld verfügen und Mittellose, die nie einen Einkauf machen können oder Besuch haben.

Auch im Knast lebt mancher auf Kosten Anderer.
Andererseits versucht auch die Anstalt, die Gefangenen zu spalten und Gerüchte zu verbreiten. Verhalte dich - den dortigen Umständen angepasst - so wie draußen, wo du auch nicht jeden vertraust, auch nicht jedem deiner Gegner siehst. Auch für die politische Solidarität gilt - mit einigen Abweichungen - drinnen das Gleiche wie draußen. Es gilt aber einige besondere Gesichtspunkte, die man beachten muss. Obwohl man dicht aufeinander hockt, weiß man vom Anderen nur das, was er selbst erzählt. Die Gleichartigkeit der äußeren Situation, aber auch das Aufeinanderangewiesensein bewirkt häufig, dass man sein eigenes, vieleicht berechtigtes Misstrauen wie Verrat empfindet. Wenn er gut ist, kannst du mit ihm reden oder er versteht es auch so. Wenn nicht, ist Misstrauen jedenfalls nicht verkehrt.

Es passiert immer wieder, dass Inhaftierte sehr schnell auf andere Gefangene hereinfallen, weil sie auf deren politische Sprüche und Verbalradikalismus hereinfallen. Wer beim Hofgang „Deutschland Er...“ schreit, ist noch nicht unbedingt ein Kamerad. Vielleicht will er „nur“, dass du ihm etwas von deiner Ration abgibst oder ihm einen Anwalt besorgst. Das kannst du ruhig tun. Aber bedenke, dass er vielleicht einen Tag später bei einem Anderen „Rotfront“ ruft. Dieses Misstrauen quält einen und gehört zu den schwierigsten Problemen im Knast. Einerseits kommt man sich dabei sehr blöde vor, andererseits muss man sich im Klaren sein, dass der Mitgefangene ein Spitzel sein kann, der sich durch Verrat die Aussetzung seiner Resthaftstrafe erschleichen will. Es bleibt uns nicht anderes übrig, als uns mit der Problematik von Verrätertum, Verräter und Provokateuren allgemein zu beschäftigen.
All diese Erscheinungen sind nicht auf den Knast beschränkt:
Im Grunde ist es nicht anders als im Betrieb, in der Schule oder der politischen Gruppe. Hier wie dort ist Verfolgungswahn, der in jedem den Agenten sieht, ebenso gefährlich wie unüberlegte, schulterklopfende Verbrüderung. **Wenn du draußen kein Prahlhans bist, wirst du drinnen auch nicht den Mund aufreißen. Du bist nicht darauf angewiesen, Anderen mit Worten zu imponieren. Man wird dich ohnehin nach deinem Verhalten einschätzen, nicht danach was du sagst.**

11.4.24 Dein Verhalten gegenüber den Beamten

Der Knast ist ein hierarchisch organisiertes Behördengebilde. Ganz oben ist der Anstaltsleiter, der über sich noch den Präsidenten eines Justizvollzugsamtes und darüber das Ministerium hat. Dann geht es über etwa acht bis zehn Dienstgrade nach unten bis zu den Beamten, die den uniformierten Dienst an der Zellentür und im Flur tun.

Der Knast funktioniert heute in der Regel, weil jeder vor jedem Angst hat. Jeder Beamte vor seinem Vorgesetzen. Aber auch vor seinem Kollegen, weil er ihm den Rang um die spärlich gestreuten Beförderungsstellen ablaufen kann.

Alle zusammen haben sie Angst vor der Öffentlichkeit, insbesondere vor der Presse, weil in jedem Knast so viele Ungerechtigkeiten und skandalöse Dinge passieren, dass man einen erheblichen Aufwand an Abschirmung und Verschleierung betreiben muss.

Die Angst, ständig etwas falsch zu machen, ständig von oben angeschissen werden zu können, erzeugt innerhalb des Gefängnisses eine Atomsphäre von Gereiztheit und Aggressivität, unabhängig vom Verhalten der Gefangenen. Erfahrungsgemäß legen die Beamten sich nicht mit denjenigen an, von denen sie abhängig sind, sondern sie lassen ihren Unmut an denen aus, die ihnen unterlegen sind. Das schafft ein gereiztes, feindliches Verhältnis zwischen Gefangenen und Beamten.

Das kommt letztlich wieder denjenigen zugute, deren Interesse mit Hilfe des Knastes durchgesetzt werden soll.

Da aber auch Beamte ihren Dienst möglich reibungslos und kraftsparend erledigen wollen, sind sie darauf angewiesen, das Verhältnis zu den Gefangenen nicht sehr zu strapazieren. Es kommt also zu einer Art Waffenstillstand. Dieser ist erzwungen durch die Tatsache, dass einerseits die Beamten ihren Dienst nicht ohne gewisse Kooperation der Gefangenen ableisten können und dass andererseits die Gefangenen die Leidtragenden ständiger Schikane und Maßregeln wären. Dieser Waffenstillstand ist sehr zerbrechlich, weil jede Veränderung des Gleichgewichtes, etwa durch Einschränkung der Rechte der Häftling oder Verschärfung der Dienstpflichten der Beamten, zu gemeinschaftlichen Aktionen der einen wie der anderen Seite führen können. Diese gefährdet letztlich einen Strafvollzug wie er von den Herrschenden gewünscht wird.

Die Tatsache, dass ein solcher Waffenstillstand im Allgemeinen besteht, darf nicht darüber hinwegtäuschen, dass im Kleinen die Gefangenen täglich mit allen möglichen Schikanen und unzulässigen Maßnahmen bedacht werden. Für den einzelnen Gefangen bedeutet das, dass er sich im Verkehr mit den Beamten unauffällig korrekt verhalten sollte, solange dies der Beamte auch tut. Sobald du denkst, dass ein Beamter auf einen Privatkonflikt mit dir aus ist, musst du dich wehren. Du hast dann Anspruch auf die Mitsolidarität deiner Mitgefangenen, deines Anwaltes und anderer, die dir zu deinem Recht verhelfen können. Das gleiche gilt, wenn du siehst, wie andere schikaniert werden.

Sei dir aber immer im klaren über den Adressaten deiner Maßnahmen. Wenn der Beamte Anordnungen ausführt, die er nicht gewollt oder nicht zu verantworten hat, ist er meist nicht in der Lage, sich mit dir gegen den Anordnenden zu verbünden. Er kann schließlich aber seinen Dienst pingelig genau nehmen oder auch mal fünfe gerade sein lassen.

Wenn er sich aber mit einer Schikane gegen dich, die von oben kommt, identifiziert, dann ist die Grenzlinie klar gezogen. Der Knast funktioniert meistens so, dass derjenige, der eine besondere Anordnung trifft, etwa die Überwachung bei Nacht, Lichteinschaltung etc., diese nicht selbst ausgeführt. Der betreffende Gefangene kommt nur noch mit dem Überbringer und Ausführenden in Berührung.

Das hat zur Folge, dass sich die ganze Empörung aggressiv auf den Beamten entlädt, der eigentlich nicht verantwortlich ist. Meist ist der Beamte aber nicht mutig genug, sich offen mit dem Gefangenen zu solidarisieren oder seine Empörung zu teilen. Er steht in einem Rollenkonflikt, in dem er mit dir sympathisieren will, aber nicht darf, weil er die Anforderung ausführen muss. Sein Mut wird nicht zur Gehorsamsverweigerung reichen, aber es wäre schädlich, durch unkontrollierte Aggressivität gegen den Beamten ihm den politisch emotionalen Zugang zu dir zu verbauen.

Zeige ihm, dass du den Mut gegenüber seinen Vorgesetzten hast, den er nicht hat, obwohl ihm weniger passieren würde. Die Beamten identifizieren sich oft mit dem Stärkeren. Wenn es ihr Chef ist, mit ihm, wenn du es bist, mit dir.

Es ist klar, dass diese Darstellung sehr schematisch ist und der „gute“ Beamte zumindest in der heutigen Zeit die Ausnahme darstellt. Wenn man sich jedoch über diese Strukturen innerhalb des staatlichen Herrschaftsapparates nicht klar ist, vergibt man ein wichtiges Operationsfeld und schwächt seine eigene Position.

Du sollst kein Mitleid mit ihm haben, sondern seine Reaktion dir gegenüber realistisch auf Ursachen hin deuten, damit du dich ihm gegenüber richtig verhältst.

11.4.25 Welcher Anwalt ?

Nimm nicht einen Anwalt, der mal die eine Seite, mal die andere vertritt, der meint, bei Gericht betonen zu müssen, er sei nicht der politischen Ansicht seiner Mandanten.

Ein solcher Anwalt empfiehlt sich nicht für dich. Bei ihm besteht die Gefahr, dass er sich insgeheim, bewusst oder unbewusst, mehr mit deinem Gegner identifiziert als mit dir. Ein Anwalt, der darauf angewiesen ist, häufiger von einem Gericht als Pflichtverteidiger beigeordnet zu werden, wird nicht riskieren, die Rechte seines Mandanten auch dann voll wahrzunehmen, wenn es für das Gericht lästig ist. Ein solcher Anwalt ist, selbst wenn er diesen Vorwurf mit vielen Worten weit von sich weisen wird, käuflich. Gerade in politischen Verfahren wird der Anwalt häufig mit seinen Mandanten identifiziert. Er wird gerne von der Presse und Staatsanwaltschaft zu seinem Komplizen gestempelt. Der Anwalt weiß oder ahnt das und wird sich in irgendeiner Weise z.B. durch Erklärungen, durch sein Verhalten oder auch durch Bemerkungen in der Gerichtskantine, von dir zu distanzieren versuchen. Auch er ist politisch gesehen käuflich.

Wenn du es dir finanziell leisten kann, dann nimm dir einen Staranwalt. Er ist so groß, dass er aus der Bekanntheit deines Falles Nutzen für sich ziehen kann. Außerdem ist er reich und so über jeden Verdacht erhaben, zumindest finanziell abhängig zu sein. Man wird ihn auf Cocktail - Parties auf deinen Fall ansprechen. Aber er wird viel für dich tun. Er ist seinem Ruf etwas schuldig. Er will sich nicht blamieren und genau deshalb kann er unter Umständen nützlich sein.

Viele sagen, der Anwalt sollte möglichst politischer Gesinnungsgenosse sein. Für viele ist die Frage, wer wirklich Kamerad ist, nicht leicht zu beantworten. Angesichts der vielen Fraktionen, Organisationen und Meinungen im nationalen Lager ist das ein schwammiges Kriterium. Wichtig ist, dass der Anwalt deine Interessen vertritt, Deine Rechte wahrt und dich verteidigt. Du musst prüfen, ob er das tut, weil er reich werden will oder weil er Durchblick hat. Wenn er Durchblick hat, dann will er nicht reich werden. Dann ist er engagiert auf der Seite derjenigen, denen ihre Rechte genommen werden, nur weil ihr Einsatz dem Volk und Land gilt. Er vertritt nicht die Klienten, die ihn gut bezahlen, sondern die, auf deren Seite er steht. Er arbeitet, so gesehen, nicht für Geld.

Vergewissere dich rechtzeitig bei deinen Kameraden oder bei Gefangenenhilfsorganisationen, ob in deiner Umgebung, in deiner Stadt oder in der Nähe solch ein Anwalt ist. Es ist ratsam, sich mit dieser Frage nicht erst zu befassen, wenn man in der Klemme sitzt. Meist drängt dann die Zeit. Du kannst eine Menge Energie und Nerven sparen, wenn du vorher schon weißt, wer dir helfen kann.

Viele meinen, man dürfe Anwälte nicht mit „unwichtigen“ oder gar „unpolitischen Sachen“ des täglichen Lebens von den wichtigen, großen Fällen abhalten. Wenn der Anwalt Durchblick hat, dann weiß er, dass Unterdrückung und Umerziehung in allen Bereichen aktiv ist.

Unterdrückung funktioniert im Wesentlichen dadurch, dass die eigenen Leute Niederlagen haben, weil sie sich schwach fühlen.

11.4.26 Kosten für den Anwalt

Versuche mit dem Anwalt ein Gestgeld auszuhandeln. Sage ihm wie viel Geld du zur Verfügung hast und bitte ihn darum, dich für einen Festbetrag zu verteidigen. Schlage vor für die Rechtszüge z.B. 1000 Euro zu veranschlagen. Die meisten Anwälte gehen darauf ein. Schnell könnten die Kosten immens steigen und Du bekommst nach deiner Freilassung eine sehr hohe Rechnung. Mit dem Festbetrag kann dir das nicht passieren.

Solltest du sehr knapp bei Kasse sein, versuche ob du die Kosten auf den Staat abwälzen kannst. Du oder dein Anwalt können Prozesskostenbeihilfe (PKH) beantragen. Wenn du kein Einkommen

hast, Arbeitslos oder von Sozialhilfe lebst, solltest du unbedingt PKH beantragen. Ein Formblatt ausfüllen, bei Gericht beantragen und der Staat übernimmt einen Prozentsatz deiner Anwaltskosten. Oftmals sogar fast 70 bis 90
Versuche mit dem Anwalt alle Fehler aufzudecken die Beamte bei der Festnahme, Durchsuchung usw. gemacht haben. Viele Kameraden sind aus der Haft wieder entlassen worden, weil übereifrige Polizeibeamte und Staatsanwälte FFormfehlergemacht haben und somit rechtswidrig eine Inhaftierung angeordnet haben. Wenn ihr die Fehler dem Richter glaubhaft darlegt wird er schnell seinen Haftbefehl fallen lassen und ihr werdet aus der Haft entlassen.

Der Fehler der oftmals von Behörden gemacht wird ist, dass du zu übereifrig bei einem Verhör in die Mangel genommen wurdest und unter psychischem Druck zur Aussage „gezwungen wurdest“. Kannst du das beweisen bist du so gut wie frei. Bedenke dass du alle Aussagen, mit einem guten Grund, widerrufen kannst. Als Gründe könntest du Psychodruck oder Alkoholeinfluss nennen. Sobald du wieder auf freiem Fuß bist, versuche den Alltag, z.B. deine Arbeit wieder herzustellen damit du nicht in einem „Haftloch“ steckst und Monate brauchst um dich auf den Alltag im „großen Knast“ einzustellen

11.4.27 Prozesskostenbeihilfe

Über die Prozesskostenhilfe (PKH) (früher als „Armenrecht“ bezeichnet) kann gem. §§ 114 ff. ZPO einkommensschwachen Personen eine finanzielle Unterstützung zur Durchführung von Gerichtsverfahren gewährt werden. Prozesskostenhilfe kommt in Verfahren vor den Zivil-, Verwaltungs-, Arbeits- und Sozialgerichten in Betracht, wenn eine Verfahrenspartei nicht in der Lage ist, die Anwalts- und Gerichtskosten für den Prozess aufzubringen. In Strafverfahren kann nur Nebenklägern oder Adhäsionsklägern Prozesskostenhilfe gewährt werden. Die Prozesskostenhilfe trägt der Staat. Sie ist eine spezialgesetzlich geregelte Einrichtung der Sozialhilfe im Bereich der Rechtspflege und dient der Umsetzung der Rechtsschutzgleichheit. In bestimmten Verfahren nach dem FamFG wird die Prozesskostenhilfe als Verfahrenskostenhilfe (VKH) bezeichnet.

11.4.28 Dein Verhalten gegenüber Polizei und Justiz - Zusatzblatt

Der Umgang mit der BRD - Exekutive wird in mehreren Schriften ausreichend beschrieben. Die Praxis ist jedoch, dass scheinbar unproblematische Handlungsabläufe gar nicht so unproblematisch sind - vor allem dann, wenn man unter Zeitdruck handeln muss.

Die nachfolgenden Informationen sollen den Handlungsablauf folgender Situation skizzieren:

„Kamerad Winston wird morgens unsanft geweckt, Vor seinem Bett stehen mehrere Beamte des BRD - Systems, verhaften ihn, durchsuchen seine Wohnung. Während der Fahrt zum Revier erfährt Winston was ihm vorgeworfen wird. Zum Glück kann er noch eine Nachticht an seine Freundin Julia senden ...“

WELCHE INFORMATIONEN BRAUCHT JULIA VON WINSTON ?

Wo wird Winston festgehalten?
Was wird Winston vorgeworfen?
Wann wurde Winston verhaftet?
Möchte Winston einen Anwalt einschalten?
Wann soll Winston dem Haftrichter vorgeführt werden?

Nachdem Julia die nötigen Informationen von Winston erhalten hat sucht sie die Anwalt - Notrufnummern für Strafrecht aus ihrem Notizbuch. Sie wählt die erste Nummer - Telefon aus. Gut das sie sich mehrere Anwalt - Notrufnummern aufgeschrieben hat. Die zweite Nummer - es geht jemand ran, leider ist er gerade unterwegs und schafft es aufgrund der Entfernung nicht mehr

rechtzeitig zu Winston zu kommen. Die dritte Nummer - endlich, Julia bekommt Hilfe.

WAS SOLLTE JULIA BEIM GESPRÄCH MIT DEM ANWALT BEACHTEN ?

Julia weiss nicht weswegen, sondern nur was Winston vorgeworfen wird. Sie erinnert sich das Winstons Aktionen durchgeführt hat welche unter diesen Strafbestend fallen. Sie weiss jedoch nicht ob er wegen dieser Aktionen verhaftet wirde. Da sie aus dem privaten Umfeld von Winston kommt muss Julia damit rechnen das ihr Telefon angezapft wird. Deshalb erzählt sie dem Anwalt nichts von der Aktion! Ohnehin währe es nur einer Vermutung.

WELCHE INFORMATIONEN BRAUCHT DER ANWALT ?

Wo wird Winston festgehalten?
Den Namen von Winston.
Die Adresse von Winston.
Das Geburtsdatum von Winston.
Das Revier in dem Winston festgehalten wird.
Der Vorwurf der Winston gemacht wird.
Wann Winston verhaftet wurde.
Wann Winston dem Haftrichter vorgeführt werden soll.
Den Namen von Julia (bzw. der Eltern von Winston).
Die Telefonnummer von Julia (bzw. der Eltern von Winston).

Spätestens nach dem Gespräch mit dem Anwalt sollte Julia den engen Kameradenkreis von Winston informieren damit sie ggf. ihre Wohnung auf einen Besuch vorbeireiten können. Julia sollte die Zeit natürlich auch nicht ungenutzt vergehen lassen.

11.4.29 Polizeikonzepte aufdecken!

Zugegeben, der Leak ist schon eine Weile her. Nach wie vor bietet das Dokument aber Einblick in die Strategien von Polizei, Justiz und Verwaltungsbehörden, die einem zum Teil den Atem stocken lassen. Das hier veröffentlichte „ganzheitliche und länderübergreifende strategisch-taktische Rahmenkonzept zur Bekämpfung der Rockerkriminalität“ betrifft uns als Nationalisten zwar nicht unmittelbar. Die taktischen Konzepte werden aber auch uns gegenüber angewandt.

So heißt es zum Beispiel über Hausdurchsuchungen (S. 24):
Durch diese Maßnahme wird den Betroffenen verdeutlicht, dass sie sich keineswegs ... im rechtsfreien Raum bewegen. ... Neben Durchsuchungsmaßnahmen zur Strafverfolgung sind bei Vorliegen polizeirechtlicher Voraussetzungen konsequent Wohnungen, Fahrzeuge ... zu durchsuchen. [Hausdurchsuchungen] entfalten eine nachhaltige Wirkung [und] sind auch ein wirksames Mittel, um Zeichen zu setzen.

Angemerkt sei, dass sog. „polizeirechtliche Voraussetzungen“ zur Beschlagnahme bereits vorliegen, wenn der Beamte irgend einen Verdacht hat. Dieser besteht regelmäßig, wenn der Beamte vor einem Laptop oder einem Kleiderschrank oder sonst einem Gegenstand steht, den er gerne haben will. Da ist es kein Wunder, dass mit solchen Maßnahmen der Willkür Tür und Tor geöffnet werden.

Das polizeiliche Vorgehen, das die Grenze der Schikane längst überschritten hat, treibt mittlerweile derartige Blüten, dass u.a. nicht mehr davor zurückgeschreckt wird, morgens um sechs per Rammbock die Wohnung zu stürmen, Haustiere in der Wohnung zu erschießen oder (legale) massive Waffenschränke gefließte Wohnungstreppen hinunterzuwerfen, so dass die Betroffenen (oft Familien mit Kindern) nicht nur einen massiven Sachschaden zu beklagen haben, sondern oft auch mit

psychischen Traumata zurück bleiben.

Diese Vorfälle klingen extrem, stellen jedoch ausdrücklich keine Einzelfälle mehr dar. Die Auswirkungen derartiger Polizeieinsätze sind im Gegenteil ausdrücklich gewollt, da es längst nicht mehr um den Erhalt der Rechtsordnung geht, sondern um die Einschüchterung und wirtschaftliche und psychische Vernichtung potentieller Gegner der Etablierten. Gespeichert in einer PDF Datei kannst du das Polizeiliche Dokument beim Verfasser dieses Artikels, dem Infoportal Schwaben und natürlich bei uns im Menüpunkt Material herunterladen.

11.4.30 Ein Rahmenkonzept zur Bekämpfung der Rockerkriminalität

Wird mithilfe der Medien das subjektive Sicherheitsempfinden der Bevölkerung manipuliert und instrumentalisiert?

Es ist auffällig, wie viele Einsätze deutsche Behörden derzeit gegen Rocker, vor allem gegen die Hells Angels, führen. Das Verhältnis zwischen Rockern und Behörden war schon immer schwierig - aktuell aber ist das Verhalten mancher Behörden so ungewöhnlich, dass auch in ausländischen Medien dies Phänomen nachgefragt wird: Razzien, Durchsuchungen und Verhaftungen gehen parallel zu Verboten und Selbstauflösungen von Hells Angels-Chartern (Ortsgruppen).

Zwei Schwerpunkte bei Rockereinsätzen: Seit Mai 2012, seit April 2010
Zwar ist die ganz große Aktivität seitens der Behörden neu und dürfte mit dem Prozess in Kiel im Mai dieses Jahres gegen den ehemaligen Legion 81-Rocker Steffen R. zusammenhängen. Der hatte zahlreiche Hörensagen über die Hells Angels wiedergegeben, deren wohl wichtigste - der ehemalige Hannoversche Rocker Frank Hanebuth als inoffizieller Deutschlandchef und Auftraggeber für einen Mord, eine eingemauerte Leiche in einer Lagerhalle in Altenholz, eine angebliche Folterkammer in Kiel - sich in Luft aufgelöst haben. Aber noch, bevor sie überprüft worden waren, wurde der Angeklagte zu einer außerordentlich milden Strafe für seine Verbrechen verurteilt.

Eine schon deutlich gesteigerte Aktivität von Behörden gegen die Hells Angels lässt sich jedoch auch schon seit Längerem - genauer: Seit dem Frühjahr 2010 - nachweisen. Deutlich zeigt sich dies an Vereinsverboten und Selbstauflösungen von Hells Angels Chartern in Deutschland: Im Oktober 1983 war der Charter Hamburg verboten worden, im Januar 2001 Düsseldorf. In jüngerer Zeit erst Flensburg (April 2010), dann Borderland (Pforzheim) und der Unterstützerclub Commando 81 Borderland (Juni 2011), danach Frankfurt und Westend (September 2011). Im Jahr 2012 zuerst Kiel (Januar), im April Cologne, im Mai Berlin City und Singen, im Juni Southport, Potsdam, Hannover und West Side (Bremen).

Kurz: In den 1980er Jahren wurde ein Charter geschlossen, in den 1990er Jahren keiner, in den Nuller Jahren wieder einer. Das ist nicht viel. Aber seit 2010, also innerhalb von nur zweieinhalb Jahren, verschwanden elf Charter von der Bildfläche.

Zwar haben sich einige Charter wie etwa Hannover oder West Side selbst aufgelöst. Man kann dafür mehrere Gründe vermuten: Wenn ein Verein nicht mehr existiert, kann er nicht verboten und das Vereinsvermögen nicht beschlagnahmt werden. Oder die Rocker wollen weiterhin Hells Angels sein und sich in einem anderen Charter zusammenschließen, was schwierig wäre, wenn sie zu einem verbotenen Charter gehört hätten.

Also dürften auch Selbstauflösungen auf äußeren Druck zurückzuführen sein.

Außerdem stehen den Verboten und Auflösungen zahlreiche Neugründungen gegenüber: Der erste Hells Angels-Charter in Deutschland wurde im Jahr 1973 in Hamburg gegründet (und nach zehn Jahren verboten). Inzwischen ist Stuttgart der älteste - 1981 gegründet - und Nummer Zwei, Ber-

lin, gibt es seit 1990. Bis 1998 gab es wohl gut ein halbes Dutzend Charter in Deutschland. Im Jahr 1999 kamen 14 neue dazu - fast alle durch den Übertritt der Rockergruppe Bones. In den Nuller Jahren kamen 22 Charter hinzu und seit 2010, also in den letzten zweieinhalb Jahren, 19. Allein vier von ihnen wurden in den vergangenen Wochen in Berlin gegründet.

Folgten die Verbote den Neugründungen? Reagierten die Behörden also auf die Rocker? Die Logik wäre: mehr Charter - mehr Straftaten - mehr Verbote. Dagegen spricht aber zweierlei: Erstens, dass in den Nuller Jahren 22 Charter entstanden, aber nur einer geschlossen wurde. Zweitens wirken zumindest manche Neugründungen (wie etwa die vier Berliner Charter Northtown, Southtown, Westtown und Easttown) wie eine Reaktion von Rockern auf Behörden - vielleicht, um diese zu provozieren. Das schließt das Erste nicht aus, passt aber nicht so recht dazu.

Auffällig ist vor allem der Beginn der Kette der Schließungen im April 2010. Konzept zur Bekämpfung der Rockerkriminalität könnte Einsatzschwerpunkt seit April 2010 erklären
Ein Dokument könnte (mit) erklären, warum Polizeibehörden seit genau diesem Zeitpunkt so viele Einsätze gerade gegen die Hells Angels durchführen.

Ein „Unterausschuss Führung, Einsatz und Kriminalitätsbekämpfung“ (UA FEK) hatte eine Bund-Länder-Projektgruppe „Bekämpfungsstrategie Rockerkriminalität-Rahmenkonzeption“ (BLPG BR-RK) eingerichtet. Ziel der Projektgruppe ist die Abstimmung des gemeinsamen Vorgehens gegen Rockerkriminalität. Sie hat ein Dokument herausgebracht, es heißt: „Bericht der Bund-Länder-Projektgruppe des UA FEK „Bekämpfungsstrategie Rockerkriminalität - Rahmenkonzeption“ [BLPG BR-RK]“. Es stammt vom Ministerium des Innern und für Sport Rheinland-Pfalz, ist gekennzeichnet als „VS - NUR FÜR DEN DIENSTGEBRAUCH (i.S. IFG nicht freigabefähig)“ und steht seit ein paar Wochen öffentlich einsehbar auf einer Website der Hells Angels. Es wirkt echt.

Das 64-seitige Dokument beinhaltet die „Entwicklung eines ganzheitlichen und länderübergreifenden strategisch-taktischen Rahmenkonzeptes zur Bekämpfung der Rockerkriminalität“ und gibt den Stand vom 7. Oktober 2010 wieder.

Seine Verfasser begründen die Ausarbeitung eines solchen Rahmenkonzeptes damit, dass es „bundesweit wiederholt zu gewalttätigen Auseinandersetzungen bis hin zu Tötungsdelikten zwischen rivalisierenden Rockergruppen“ (S. 4) gekommen sei, und dass mit zunehmenden Aktivitäten der Gruppierungen die Gefahr einer Eskalation der Rockerkriminalität steige. Sie nehmen auch Bezug auf ein tragisches Ereignis vom 17. März 2010. An diesem Tag erschoss ein Mitglied der Hells Angels in Rheinland Pfalz einen Polizisten.

Der Rocker war zu Hause, als ein SEK kam und seine Wohnung betreten wollte. Als die Beamten seine Wohnungstür öffnen wollten, schoss der Rocker zweimal durch die geschlossene Tür und traf einen der Polizisten so unglücklich, dass dieser trotz schusssicherer Weste sein Leben verlor. Der Rocker wurde durch den Bundesgerichtshof freigesprochen, der die Verantwortlichkeit für den Vorfall bei der polizeilichen Einsatzleitung sah: Der Hells Angel hatte gesagt, er habe einen Überfall von Bandidos befürchtet.

Im Bericht heißt es zu den Auseinandersetzungen zwischen Rockergruppen und dem Tod des Polizeibeamten: „Vor dem Hintergrund dieser Entwicklung gilt es einen polizeilichen Schwerpunkt zu setzen, die bundesweit vorliegenden Bekämpfungsstrategien konzeptionell zu bündeln und darüber hinaus auch andere Behörden und Stellen durch Kooperation mit einzubeziehen.“ (S. 4) Warum und wie dies geschehen soll, wird auf 64 Seiten ausgeführt. Diese Rahmenkonzeption besteht aus elf Teilen: Vorbemerkung (I), Lagebeschreibung (II), (Einsatz-)Organisation (III), Informationsmanagement, Ermittlungen und Geheimhaltung (IV), Zusammenarbeit (V), Öffentlichkeitsarbeit (VI), Prävention (VII), Aus- und Fortbildung (VIII), Wirkungszusammenhänge (IX), Weitere Hinweise der Projektgruppe (X) und schließlich Fortschreibung (XI). Der Schwerpunkt des Berichtes liegt

in den Ausführungen zur Einsatzorganisation.

An dieser Stelle sollen nur zwei Aspekte herausgegriffen werden: Erstens die Rolle der Polizei, zweitens die Rolle der Medien.

Zunächst zur Rolle der Polizei. In der Akte steht: „Die „BLPG BR-RK“' misst der Rolle der Polizei bei der Bekämpfung von Rockerkriminalität vor dem geschilderten Gesamthintergrund grundsätzliche Bedeutung zu“ (S. 7). Die beiden Ziele der Projektgruppe sind „die Erarbeitung präventiver und regressiver Bekämpfungsstrategien unter Einbeziehung anderer zuständiger Stellen“ sowie „Information und Beratung der Politik ... insbesondere im Hinblick auf Rechtsfortentwicklung.“

Gleich dieser Beginn wirft die Frage auf, ob es die Rolle der Polizei sein darf, Lobbyarbeit für „Rechtsfortentwicklung“ zu treiben: Wird dadurch nicht die Gewaltenteilung infrage gestellt? Das Konzept empfiehlt, ein Verbotsverfahren nach dem Vereinsgesetz zu prüfen, „sofern Ermittlungen gegen Rockergruppen zu dem Ergebnis geführt haben, dass die Aktivitäten des Clubs auf die planmäßige Begehung von Straftaten ausgerichtet sind, dass der Club Straftaten einzelner Mitglieder im Clubinteresse duldet, fördert oder deckt oder dass die Aktivitäten des Clubs gegen die freiheitlich demokratische Grundordnung ausgerichtet sind“ (S. 60).

Hieran ist natürlich nichts auszusetzen. Im Gegenteil. Allerdings war dies auch schon vorher möglich.

Außerdem wird eine lange Liste „taktischer Maßnahmen“ aufgezählt (S. 13 - 25), die nicht nur der Ermittlung von Straftaten dienen, sondern auch der Überzeugung von Justiz und Ordnungsbehörden von der polizeilichen Sicht (S. 17), oder der einfachen Störung von Rockergruppen. So seien Gewerbeanmeldungen „intensiv“ zu prüfen (S. 48), oder die sehr professionell gesicherten Vereinshäuser sollten von Bauordnungsämtern „restriktiv geprüft“ werden (S. 48). - Vielleicht mussten die ehemaligen Mitglieder des früheren Bremer Charters „West Side“ deswegen kürzlich ihr altes Clubhaus räumen - nach Angaben des Weser-Kuriers hat das Bauressort die Nutzung ihres Gebäudes für Versammlungen und Veranstaltungen untersagt.

So fragt sich, ob dies Konzept nun eigentlich nur darauf zielt, die polizeilichen Ermittlungen zu unterstützen, oder ob es nicht (zumindest im Nebeneffekt) die Auffassung durchsetzen soll, dass Rockergruppen wie die Hells Angels grundsätzlich kriminell sind und verboten gehören.

Die Legitimität dieses Konzeptes bestreitet denn auch der Rechtsanwalt Michael Karthal, der für den verbotenen Charter HAMC Frankfurt die Verbotsverfügung des Hessischen Innenministeriums anficht. In seiner Klagebegründung schreibt er mit Bezug auf dieses Konzept: Einziges Ziel sei, „die Innenministerien zu veranlassen, Vereinsverbote auszusprechen.“ Diese unterliegen nämlich „nicht der strengen Nachweispflicht für strafrechtliche Verurteilungen [...], sondern ein Zurechnungszusammenhang zwischen den Taten einzelner und mehrerer Mitglieder und dem Verhalten der übrigen Vereinsmitglieder“ genüge.

Natürlich: Wenn ein, wie Rechtsanwalt Karthal schreibt, „Zurechnungszusammenhang zwischen den Taten einzelner und mehrerer Mitglieder und dem Verhalten der übrigen Vereinsmitglieder“ nachgewiesen werden kann, und dies Grundlage für ein Vereinsverbot ist, dann kann ein Vereinsverbot durchaus im Sinne der Bevölkerung sein. Es fragt sich aber, ob die hohe Anzahl der Vereinsverbote nahelegt, dass so ein Zurechnungszusammenhang regelmäßig besteht? Wenn ja, dann folgt unvermeidlich eine weitere Frage: Besteht dieser Zusammenhang erst seit April 2010? Der Tod des Polizisten ist tragisch, aber kann man daraus bei so vielen Chartern bundesweit auf diesen Zusammenhang schließen?

Karthal zieht den umgekehrten Schluss: „Der von nun an verfolgten polizeilichen Strategie ist insbesondere die Erkenntnis geschuldet, dass der strafrechtlich geforderte Nachweis einer organi-

sierten kriminellen Vereinigung trotz umfangreicher und zielgerichteter Ermittlungen nicht geführt werden konnte. Als dennoch sanktionierendes Instrument für eine nicht nachgewiesene organisierte Strafrechtswidrigkeit der Vereinigungen haben die Polizeibehörden zur Beseitigung des Vereinslebens die den Grundrechtsschutz einschränkenden Verbotsverfügungen erkannt."

Ein zweiter wichtiger Aspekt im Rahmenkonzept ist die Rolle der Medien bzw. das Konzept der Presse- und Öffentlichkeitsarbeit. Sie hat eine: „zentrale Bedeutung." (S. 8) Ihr ist sogar ein ganzes Kapitel gewidmet (Kapitel VI, S. 55 - 58), denn: „Die Medien beeinflussen ganz überwiegend die Wahrnehmung der Öffentlichkeit und damit auch die Akzeptanz und Wirksamkeit polizeilicher Maßnahmen." (S. 55). Ziel der Öffentlichkeitsarbeit ist außerdem, die „Kooperationsbereitschaft der Bevölkerung" zu erhöhen (S. 55) und - erstaunlicherweise - die „[u]mfassende Information und Sensibilisierung aller Polizeibeamtinnen und Polizeibeamten" (S. 55). Informiert die Polizei ihre Mitarbeiter über öffentliche Medien?

Presse- und Öffentlichkeitsarbeit ist genannt als Teil der polizeilichen Taktik und bildet den Abschluss unter den taktischen Leitlinien: „Eine einsatzbegleitende und anlassunabhängige Presse- und Öffentlichkeitsarbeit macht das konsequente Vorgehen der Polizei deutlich, entmythologisiert die OMCG (Outlaw MotorCycle Groups) und berücksichtigt dabei ausgewogen die subjektive Sicherheitslage." (S. 14).

Auffällig ist gerade im Zusammenhang mit taktischen Leitlinien zweierlei: Erstens soll die Öffentlichkeitsarbeit anlassunabhängig sein. Das heißt: Man braucht keinen Anlass, um über Rockergruppen zu informieren. Kein Verbrechen, kein Vergehen, nichts. Zweitens soll die Presse- und Öffentlichkeitsarbeit die subjektive Sicherheitslage der Bevölkerung berücksichtigen: also Empfindungen, nicht Fakten. Nun ist natürlich wünschenswert, dass die subjektive Befindlichkeit der Bevölkerung berücksichtigt wird. Es ist sogar lobenswert.
Es fällt jedoch auf, dass polizeiliche Presseinformationen, etwa über Razzien, in der Tat häufig ungenau und subjektiv sind: Es wird oft von „Drogenfunden" berichtet, aber vielleicht sind es bloß 20 Gramm Marihuana? „Verurteilungen" können sich auf Verbrechen beziehen - aber ebenso gut auch auf Verkehrsvergehen. „Messer" können auch Küchenmesser sein.

Eine angemessene Angst vor Kriminalität übt eine Schutzfunktion aus. Aber wenn solch eine Angst nicht angemessen ist, mindert sie die Lebensqualität der Verängstigten. Nun berichten sogar Polizisten, dass die Pressestellen der Polizei jene Meldungen und Informationen, welche die Bevölkerung ängstigen könnten, häufig nicht veröffentlichten. Warum ist dies in Bezug auf Rocker so offensichtlich anders?

Das Rahmenkonzept weckt den Eindruck, dass Vereinsverbote angestrebt werden, weil man den Hells Angels nicht nachweisen kann, dass es sich bei ihnen um eine kriminelle Vereinigung handelt. Wenn daher Vereinsverbote zweite Wahl gegenüber strafrechtlichen Verurteilungen sind, und wenn an Vereinsverboten Folgendes von Vorteil ist: „Das Verbot qualifiziert den Rockerclub öffentlich als kriminell." (S. 63): Dann stellt sich die Frage, ob hier nicht mithilfe der Medien das subjektive Sicherheitsempfinden der Bevölkerung manipuliert und instrumentalisiert werden soll.

11.5 Wir bilden Bezugsgruppen

Wir fahren auf Demonstrationen, Kundgebungen und zu Aktionen. Immer mehr oder weniger mit den gleichen Leuten oder alleine. Diese Leute zu organisieren, ist das Anliegen der Bezugsgruppentaktik, welche auf den folgenden Seiten erklärt wird. Weder vollständig, noch führend wollen wir einige Ideen geben. Passt diese auf eure Situation vor Ort an und ergänzt sie nach Belieben. Bleibt im Kopf genau wie auf der Straße immer in Bewegung!

11.5.1 Warum eine Bezugsgruppe?

Der Einzeltäter
Du gehst alleine auf Demos und lernst dort zwar Leute kennen, jedoch entscheidest du dich meist spontan irgendwohin zu fahren. Von Aktionen erfährst du über das Netz und wenn es dann mal passt, gehst du einfach hin. Bisher hattest du vielleicht noch keine großen Probleme oder vielleicht sogar schon erste Zusammenstöße mit Gegendemonstranten.

Die Kleingruppe
Ihr seid schon immer mal ein paar Leute, die zusammen fahren. Manchmal halt mehr, manchmal weniger. Eigentlich kann auch jeder alleine an- und abreisen und manchmal passiert das sogar. Spontan geht ihr direkt nach Demo noch was trinken oder haut euch irgendwo anders die Hörner ab. Wer kein Bock hat, reist eben schon alleine ab oder geht woanders hin. Natürlich passt ihr ein bisschen aufeinander auf, aber so wirklich umsichtig seid ihr nicht. Die Abreise nehmt ihr sowieso auf die leichte Schulter, Hauptsache nachhause kommen!

Die Probleme
Eine Demo hat einen Zweck. Zu allererst möchten wir auf ein bestimmtes Thema hinweisen oder unseren Unmut ausdrücken. Jeder, der jemals mit der Planung einer größeren Aktion zu tun hatte, weiß: **Organisation ist alles.** Diese zieht sich nicht nur durch die Reihe der Veranstalter, sondern auch durch das System der Repression, Presse, Antifa und der „Bürgerlichen“. Diese haben Routine im Kampf gegen die nationale Bewegung. Diese zeigen wir folgend kurz auf:

Die Repression
Polizei und Justiz haben ein breites Spektrum an Methoden zur Einschüchterung und Überwachung. Teilnehmer einer Demonstration werden meistens rechtswidrig und willkürlich durchsucht, festgehalten oder schon auf der Anreise drangsaliert. Selbstverständlich ist der Einsatz der Ordnungsmacht vollkommen hierarchisch von oben bis unten durchgeplant. **ZIVILPOLIZISTEN beobachten die An- und Abreisenden und sind auch auf Demonstrationen zugegen. Sie sammeln Informationen und Gesichter, am liebsten sehen diese auch gleich wer wen kennt. Einzelpersonen können schnell misstrauisch von den anderen Kameraden begutachtet werden.** Auch sprechen Zivis sehr gerne Einzelpersonen auf der Abreise an - diese haben dann keine Gruppe, die Rückhalt gibt. KAMERAWAGEN (KaWa) und KAMERAPOLIZISTEN (KaPo) versuchen durch Filmen einzuschüchtern und euch zu verängstigen von euren Rechten Gebrauch zu machen. Der Umgang mit diesen sollte unbedingt in der BG besprochen werden!

Die Presse
bekommt, je nach Polizeipressestelle und Kontakten, früher oder später Wind von angemeldeten Aktionen und ist mit Fotografen und Journalisten in nächster Nähe zur Demo. Diese fotografieren im Fall der repressiven Presse Personen und Gruppen zum Zweck der späteren Diffamierung und Sammlung von Daten ab. Die bürgerlichen Medien sind ebenso organisiert und vernetzt. Nicht selten positionieren diese sich auf Balkonen und Dächern mit Teleobjektiven um trotz der Entfernung Portraitaufnahmen zu machen. Die regionale, meist ungefährlichere, Presse handelt etwas weniger professionell. Sie brauchen nur ein paar Bilder für das nächste Käseblatt und können durchaus auch für Stellungnahmen nützlich sein. (Siehe Leitfaden der NaSo-Ried zum Thema Pressemitteilung verfassen)

Die Antifa
hat sich seit dem Aufstreben der Nationalsozialistischen Bewegung in den 1930er Jahren nur einem verschrieben:**Kampf mit allen Mitteln und an allen Fronten gegen jede nationale, konservative oder patriotische Organisation und Gruppe. Angefangen bei Sportgruppen, welche anreisende Nationalisten abfangen um ihnen massiv körperlichen Schaden zuzufügen, über Unterstützer in den Landtagen die ihnen parlamentarisch den Rücken**

frei halten bis hin zu ganzen Horden an Anwälten an der juristischen Front. Neben diesen Erscheinungen nutzen auch Teile der Antifa die Methode der BGs um sich zu organisieren und zu vernetzen. Antifaschisten sehen sich selten als feste Einheit, mehr als loser Bund an - dort liegen Stärken und Schwächen. Sie können gut geplant, trainiert und vorbereitet insbesondere bei Großaufmärschen wie dem TRAUERMARSCH DRESDEN effektiven Schaden anrichten. Die Antifa ist antidemokratisch, eine breite Masse gilt als extrem gewaltbereit und bezeichnet sich selbst als kommunistisch.

Die Bürgerlichen
sind in Vereinen, „demokratischen“ Parteien oder sonstigen Grüppchen vernetzt. Zur Imagepflege gehen diese zusammen mit Gewerkschaften auf die Straße um von ihrer eigenen Unfähigkeit abzulenken und wenigstens im Kampf gegen eine Minorität zu bestehen. Ihr Laufbursche sowie Prügelknabe ist die Antifa, diese unterstützen sie auch nicht zu selten durch indirekte Versorgung. (Essensstände, Rückendeckung, ...).Viele ALT 68ER und Teilnehmer der FFriedensdemonstrationenüben sich heute als Lehrling und Schutz für die junge Generation an gewaltbereiten Antifaschisten.

Dieser Probleme bewusst, kann es nur eine Frage geben: Wieso organisieren wir uns nicht [4]?

Für den EINZELTÄTER liegt die erste Priorität auf der Suche nach Kontakten. Du brauchst Menschen, denen du vertrauen kannst. Auf Demos kann es zu Angriffen und Übergriffen kommen, außerdem müssen Inhalte trotz der Repression nach außen getragen werden. Alleine begibst du dich in Gefahren, die eigentlich leicht zu umgehen wären, wenn du dich in eine Gruppe einfügst oder selbst Leute ran holst.

Hast du eine KLEINGRUPPE von einer Handvoll oder mehr Kameraden, musst du entscheiden, welchen Zweck eure Aktionen haben. Ihr solltet euch zumindest auszugsweise Ideen aus dieser Broschüre zu Herzen nehmen und über eine Umsetzung nachdenken. Ein Ansatz zur Organisation ist die autonome Bezugsgruppe.

11.5.2 Was ist eine Bezugsgruppe?

Die Bezugsgruppe kann für viele eine sinnvolle Organisationsform sein. Sie bietet Schutz bei Übergriffen, Sicherheit auf der An- und Abreise und zusätzlich eine starke Dynamik.

Auf der Aktion könnt ihr euch darauf verlassen, dass sich jemand um euer Wohl kümmert wenn ihr festgenommen werdet oder körperlichen Schaden davon tragt. Repressionen kann in einer BG vorgebeugt werden, da ihr entschlossen auftretet und euch gegenseitig z.B. bei wahllosen Festnahmen schützt.

11.5.3 Grundlagen

Zusammensetzung
Mehr als 15 Personen machen für eine Bezugsgruppe nicht sehr viel Sinn, lieber solltet ihr diese Gruppe dann in zwei kleinere Gruppen unterteilen. Je mehr Leute, desto höher auch die Gefahr von Spitzeln.

Erste Grundlagen
Ihr müsst euch klar werden, wieso ihr euch in einer Bezugsgruppe z.B. für eine Demonstration organisiert. Vorher jedoch solltet ihr euch erst einmal kennenlernen und vertrauen, denn nur dann

[4] Seid auf der Hut vor Spitzeln. Macht ihr Dinge am Rande der Legalit ät, macht es allein und ohne davon irgendwo zu erzählen. Sonst werdet ihr als kriminelle Vereinigung eingestuft. Der Kampf um unser Volk verlangt eine neue Einsamkeit gegen die satanische Bosheit des Systems!

könnt ihr auch tatsächlich effektiv handeln. Mit anderen Leuten auf Demo sollte niemand unnötig Privates quatschen, aber in der Bezugsgruppe ist es wichtig, dass ihr euch kennt. Mindestens die politischen Antriebe und Ansichten müsst ihr austauschen und dann besprechen, mit welchem Ziel ihr die Aktion macht. Begebt ihr euch bewusst in die Grauzone des BRD-Rechts, sollte auch eine geistige Standhaftigkeit eurer Kameraden vorausgesetzt sein.

11.5.4 Fragerunde

Es gibt keine dummen Fragen

und erst recht keine dummen Antworten. Jeder muss offen sagen können, was er sich von der Aktion erhofft. Nur so könnt ihr auch tatsächlich etwas bewegen und euch im Falle von Repressionen und Festnahmen oder Ausschreitungen auf die anderen verlassen. Stellt euch zunächst folgende grundlegende Fragen:

Wiso gehen wir auf die Aktion?

Was wollen wir denn überhaupt bewegen? Wollen wir mit allen Mitteln einen Tiertransport verhindern oder eine Antifademo und die Aufklärung einer anderen Gruppe überlassen? Wollen wir stilvoll, bürgerlich gekleidet auftreten und ein gutes Bild abgeben, damit wir unsere Positionen nach außen vertreten können? Alles ist legitim, solange es keiner anderen Gruppe schadet. Jeder muss selbst wissen, für was er auf die Straße geht und wo er den Kampf kämpft. Seid ihr euch sicher, dass ihr eine Aktionsform durchziehen wollt, geht zur nächsten Frage

Wie weit wollen wir gehen?

Wo sind eure persönlichen Grenzen - jeder soll in einer Fragerunde aufzeigen wie weit er auch im Ernstfall bereit ist zu gehen. Nur so macht es Sinn, ein Mindestmaß an Aktivismus abzustecken und sich darauf zu einigen. Jeder kann sich nun bei der Aktion darauf verlassen, dass man sich vorher auf eine Grenze geeinigt hat. (Notfälle außen vor)

Welche Mittel wollen wir nutzen?

Setzen wir Fahnen ein, Transparente oder Faustis? (Klein Fahnen für die Faust). Habt ihr Ideen für anderes Material oder ist es sogar vollkommen fehl am Platz dass eure BG an diesem Tag etwas dabei hat, was sie eindeutig als Nationalisten „enttarnt"? Sprecht auch über Tabu-Material z.B. wenn ihr nichts politisches mitnehmt was genau ihr darunter versteht. Auch der Umgang mit den benutzten Materialien ist wichtig. Arbeitet ihr ein Flugblatt aus oder besorgt euch Material um auf der Anreise zu verteilen?

Gewalt?

Wir sind ständig Gewalt ausgesetzt. Der psychische Druck auf unsere Bewegung ist enorm und eine Auseinandersetzung innerhalb der Gruppe essentiell (Siehe ANGST?). Auch körperliche Gewalt kann eine Rolle spielen, wenn z.B. Sportgruppen oder aggressive Polizisten auf euch treffen. Wie weit wollt ihr gehen? Wollt ihr präventiv Gewalt anwenden um z.B. die kriminelle Antifa an der Anreise zu hindern oder positioniert ihr euch wegen eurer gewählten Aktionsform auffällig gegen Gewalt?

Angst?

Vollkommen natürlich. Jeder Mensch hat Ängste. Sprecht darüber und schafft ein offenes Klima! Niemand wird ausgelacht, weil er seine Ängste äußert. Denn wenn ihr zuvor darüber sprecht, könnt ihr ein Zusammenbruch der Gruppe während einer Aktion verhindern. Wer vorher nicht sagt, dass

er Angst hat, dem wird auch kein Einknicken während einer Aktion zugestanden. Zu solch einem Knick darf es schlichtweg nicht kommen, denn Angst kann schnell zu Feigheit werden und diese führt dazu, dass die ganze Gruppe in Gefahr sein kann. In manchen Situationen gilt es einen kühlen Kopf zu bewahren und andere nicht zu verunsichern. Trotzdem: Danach drüber reden und zugeben, dass ihr in einer bestimmten Situation schon Herzflimmern hattet, euch aber trotzdem zusammengerissen habt. Habt ihr ganz spezielle Ängste, die eine Aktion gefährden? Zum Beispiel Höhenangst, Angst vor Hunden, Platzangst, ... dann klärt die anderen darüber auf.

Umgang mit der Antifa

Wie geht ihr mit der Antifa um? Versucht ihr, dieser aus dem Weg zu gehen oder sucht ihr die Konfrontation (beides legitim, wenn die Aktionsform dies zulässt!)

Umgang mit der Polizei

Verhandelt ihr für eure Gruppe und weitere Anreisende um möglichst gute Konditionen, macht jedoch genug Druck um euch nicht verarschen zu lassen? Oder ist der Staat erklärtes Ziel eurer Aktion?

Umgang mit der Presse

Lasst ihr repressive Presseorgane wild eure Leute abfilmen oder werdet ihr diesen entschlossen zeigen, wo die Grenze ist? Nutzt ihr Schutzmaßnahmen vor Portraitaufnahmen? **Fangt ihr nach oder vor einer Aktion bewusst die kriminelle Feindpresse ab um sie zur Rede zur stellen?** Nutzt ihr die lokale Presse als Sprachrohr für eigene Stellungnahmen? Neben diesen Fragen sollte mindestens in der Bezugsgruppe Homogenität bezüglich der Weltanschauung herrschen um nicht vor Ort in grundlegenden Prinzipienfragen und Grundsatzdiskussionen zu versinken.

Weitere Vorbereitungen unter: Vorbereitung auf Aktion

Wie entscheiden wir innerhalb der Bezugsgruppe? Das ist eine wichtige Frage, denn gerade in der BG sollte niemand denken, dass seine Meinung nicht zählt. Es empfehlen sich immer ein offener Kreis und der ständige Austausch. Nach wenigen Gesprächen kristallisiert sich meistens jemand heraus, der das ganze moderiert. Es liegt an ihm, die anderen dazu zu animieren, ihre Bedenken zu äußern und Ideen vorzuschlagen. Im internen Austausch erfüllt es nicht die Ansprüche, die wir an eine BG stellen, wenn sich einzelne als Führer sehen möchten und deshalb andere Ansichten, Meinungen und Ideen unterschlagen. Gibt es niemanden, der sich eindeutig als Moderator rauskristallisiert, müsst ihr einen wählen. Zur Not mit Würfeln oder Schnick-Schnack-Schnuck. Ist das alles geklärt, könnt ihr euch an die Rollenverteilung machen.

11.5.5 Rollenverteilung

In einer BG bietet es sich an, jedem eine Aufgabe als Schwerpunkt zu geben. Folgende Rollen sollten vergeben werden. Anmerkung: Vergeben bedeutet, dass alle damit einverstanden sind und niemand Bedenken hat! Ihr könnt auch mehrere vergeben! Wortführer

Der Wortführer ist das Sprachrohr der Gruppe und gleichzeitig auch der Ansprechpartner für andere BGs. Er sammelt ständig die Meinung der eigenen Gruppe bzw. muss diese in Gefahrensituationen nach bestem Wissen schützen können.

- Anforderungen:
Redegewandt
Über Gesetze, Rechte und Pflichten geschult
Kann auch in brenzligen Situationen gut kommunizieren

Wird von der Gruppe als kompetent eingeschätzt, sodass er auch für die Gruppe etwas entscheiden kann in Notfällen

- Aufgaben:
Kontakt zu anderen Wortführer (andere BGs)
Ggf. Kontakt zum Veranstalter bzw. Ordnern
Bei Repressionen das Wort übernehmen und Kameraden über die Gesetzeslage informieren (wenn bekannt). Zur Ruhe animieren und auf das Aussageverweigerungsrecht hinweisen (siehe Broschüre „Verhalten gegenüber Polizei und Justiz“)
In brenzligen Situationen, z.B. Räumung, muss er wenn möglich mit der Gruppe entscheiden, sonst eine bedachte und sinnvolle Entscheidung treffen (Die Prinzipien wurden deshalb bewusst vorher geklärt)
Nicht gegen den Willen der Gruppe entscheiden!

Augen und Ohren / Späher (A & O, oder SPÄHER)

der A & O oder SPÄHER ist derjenige, der dem WORTFÜHRER Berichte erteilt über die Situation der Aktion und über Vorfälle sowie einzelne Personen. Er kann sich entweder innerhalb der Demo selbst befinden, oder in Absprache mit anderen Gruppen, außerhalb für alle den Späher übernehmen. Sollte die Polizei dies nicht zulassen, muss unbedingt von der Gruppe und dem Veranstalter reagiert werden.
- Anforderungen:
Flink zu Fuß, auch bei Hitze
Über Gesetze, Rechte & Pflichten geschult
Kann sich in brenzligen Situationen schnell und sinnvoll dem WORTFÜHRER mitteilen
Keine Angst vor Repressionen u. Presse

- Aufgaben:
Die gesamte Demonstration beobachten nach folgenden Gesichtspunkten:
Gibt es Schwachstellen in der Demonstration?
Wo befindet sich die Polizei und wie bewegt sie sich? (Zieht sie Kräfte zusammen? Helme auf? Provoziert sie?)
Ist Antifa in der Nähe? Wenn ja: Wie viele, welches Gewaltpotenzial?
Wird bereits blockiert und kann die Blockade geräumt werden?
Wenn er innerhalb der Demonstration ist: Sofortige Meldung bei Angriffen, Repressionen, Versuche der Polizei zu blockieren (Auch wenn andere Gruppen dies bemerken!)
Repressive Pressevertreter ausfindig machen und melden, Vorgehen wie zuvor in eurer BG besprochen?

Dem WORTFÜHRER unverzüglich kurze Meldungen geben
Sanitäter

müssen sich um das leibliche Wohl kümmern und für den Ernstfall gerüstet sein. Hierzu zählt eine Standard Ausrüstung mit einer Augenspülflasche. Entweder, er kümmert sich auch um Essen und Trinken, oder ein anderer tut dies.

- Anforderungen:
Kann erste Hilfe leisten
Hat im Idealfall medizinische Kenntnisse
Keine Angst vor Blut oder sonstigen Körperflüssigkeiten

- Aufgaben:
Auf das Wohl der Gruppe achten, Verletzte sofort behandeln oder zumindest in Schutz bringen
Um die Versorgung mit Essen und Trinken kümmern, Flaschen gleichmäßig auf Kameraden ver-

teilen. Insbesondere bei Hitze immer wieder Trinken anbieten!
Kennt die chronischen Krankheiten der Gruppe (z.B. Diabetes) und kann diese im Notfall einem DRK-Sanitäter mitteilen
- Die Versorgung
Jeder sollte genug zu Trinken dabei haben. Essen kann man auch gemeinsam vor der Aktion zubereiten, es empfehlen sich viele kleine Portionen (Brote in vielen Beuteln verteilt). So kann kurz eine kleine Mahlzeit zu sich genommen werden. Der VERSORGER oder SANITÄTER sollte die Flaschen auf alle Kameraden aufteilen, wegen des Gewichts. Die FINANZEN klärt ihr in der Gruppe, bevor es zu Streitigkeiten kommt.

Techniker
lesen mit dem Telefon z.B. die vorher ausfindig gemachten Twitter-Accounts der Gegendemonstranten oder twittern für ein Portal selbst, ohne das Ziel der Gruppe aus den Augen zu verlieren. Außerdem kümmert sich der Techniker vorher um die mitgenommenen Gegenstände wie Fahnen, Megaphone (Batterien voll?), etc. und sorgt für eine faire Verteilung dieser auf die Gruppe.

- Anforderungen:
Kann mit dem Telefon umgehen
Kann sich dem WORTFÜHRER gegenüber ausdrücken

- Aufgaben:
Technik u. Material mit der Gruppe absprechen und dann prüfen, verteilen und dafür sorgen, dass es wieder mit heim kommt Twitter, Netzseiten, Infotelefone der Gegendemonstranten checken
Kontakt zum Ermittlungsausschuss (EA), wenn vorhanden, für den Notfall sicherstellen

Navigator
- Anforderungen:
Kann Karten lesen
Kann Fahrten planen

- Aufgaben:
Schaut vor der Aktion die Umgebungskarte an und druckt diese ggf. für seine Gruppe aus
Routen der Gegendemonstranten raussuchen und mögliche Blockadepunkte besprechen
Sorgt dafür, dass die An- und Abreise reibungslos verläuft, mehr unter Vorbereitung auf Aktion
Hält die BG auf dem Laufenden, wenn es zu Abweichungen kommt und steht in gutem Kontakt mit dem SPÄHER
Kann sich dem FAHRER mitteilen

Fahrer
wenn ihr mit Autos fahrt.

- Anforderungen:
Führerschein
Kann sicher Auto fahren
Auch in Drucksituationen unfallfrei

- Aufgaben:
Stellt Sicherheit des Autos sicher (Polizeikontrollen möglich, also keine verbotenen Gegenstände im Auto!)
Transportiert die Kameraden mit Material zum Ort
Tank gefüllt, sammelt ggf. Fahrtgeld selbstständig ein

11.5.6 Vorbereitung auf Aktion

Kosten - Nutzen

Es gibt fast keine Aktion ohne Zeit- und Geldaufwand. Seid euch dessen bewusst und klärt, wie ihr das ganze finanziert. Auch den Nutzen solltet ihr abwägen und größere Aktionen ggf. zusammen mit anderen BGs durchführen damit das Geld nicht verpufft. Checkliste zur Vorarbeit

Jeder sollte über diese Punkte aufgeklärt sein. Wenn ihr nicht während der Rollenverteilung einen Zuständigen zur Informationsbeschaffung eingeteilt habt, tut dies jetzt. Geht die Liste zusammen durch, das sollte die Basis zur Vorarbeit sein.

- WER ruft zur Aktion/Demonstration auf? Unterstützt ihr diese Partei / Organisation und wie steht ihr zu dieser?
- WO findet die Aktion/Demonstration statt?
- MOTTO der Aktion/Demonstration bekannt?
- WIE findet die Aktion/Demonstration statt? (Kundgebung, ...)
- HINTERGRÜNDE recherchiert?
- WAS machen die Feinde? Gibt es schon Aufrufe?
- ANREISE mit dem Auto oder der Bahn? (Weitere siehe Anreiseplanung)
- ABREISE / SCHLAFPLATZ sichergestellt?
- WELCHE Auflagen gibt es?
- WELCHES Material nehmen wir mit, was bleibt zuhause?

Rollenverteilung
hat geklappt? Also kümmert sich auch jeder vorher schon um seine Aufgaben! Die Anderen müssen sich blind darauf verlassen können. Gebt bitte dem WORTFÜHRER Bescheid und Meldungen ab. Dieser sollte dann die ganze Gruppe informieren, wenn ihr es nicht schafft.

Du schaffst etwas nicht
Schaffst du etwas nicht alleine? Dann sag es! Teile dich sofort mit und lass dir helfen.

Anreise
Generelle Anreise-Hinweise

- Wenn Anreise mit anderen BGs Absprache über den WORTFÜHRER, ob sich die Aktionsformen angleichen lassen und Kontakt für Aktion herstellen
- Transparente können im Zug dem Abfotografieren von außen dienen und vor Steinschlag schützen. Außerdem wird eure Botschaft weit getragen
- Sobald Kontakt zu Feinden entsteht, sollte entschlossen gehandelt werden - denkt aber genau nach und begebt euch nicht unnötig in Schwierigkeiten! Antifaschisten können zwar schnell rennen, die Polizei ist meist aber auch nicht weit
- Solltet ihr auf den repressiven Polizeiapparat treffen, handelt wie besprochen. Im Idealfall könnt ihr, je nach Situation, eine Anreise bis zum Demo-Ort durch Verhandlungen ermöglichen ohne dass alle durchsucht werden. Dies ist nämlich illegal! (Vorher über Rechtslagen informieren und dann anwenden!)

- Sollte der Polizeiapparat euch behindern, sofort handeln und ggf. Namen und Dienststelle geben lassen. Dienstaufsichtsbeschwerde schreiben und nichts gefallen lassen. Sofort dem Ermittlungsausschuss (EA) melden

Generelle Aktions-Hinweise

- Kein unnötiges Geschwätz! Die Konzentration lässt nach und Beobachter können die Bewegung besser analysieren! Trefft euch privat, auf Aktion bringt ihr so das Ziel in Gefahr (Alle stehen „dumm“ rum, keiner hat mehr Antrieb etwas durchzusetzen)
- WORTFÜHRER sucht sofort die anderen Wortführer, Gruppe bleibt zusammen
- A&O verschafft sich sofort einen Überblick und kann dem WORTFÜHRER Meldung über alle aktuell wichtigen Informationen geben.
- **Bei anwesender Presse wird sofort (!) vor Portraitaufnahmen geschützt. Regenschirme ausgepackt und ggf. so vorgegangen, wie ihr es zuvor besprochen habt. (dezentes Zurechtweisen der Presse ist keine Straftat) Solltet ihr besprochen haben, nicht auf Presse zu reagieren, tut ihr das selbstverständlich.**
- Die anderen Aktionsformen vor Ort werden respektiert und nicht zu Recht gewiesen oder schlecht gemacht! Jeder hat sein Recht, so auf die Straße zu gehen, wie er einen Sinn für die Bewegung darin sieht. Gesicht zeigen heißt mutig sein, aber auch Demonstrationen durchzusetzen beweist Mut. Versteht auch, wieso manche sich eben anders geben als ihr. Vielfalt ist wichtiger als interne Repression. Lediglich eindeutig unerfahrenen Kameraden greifen wir unter die Arme und geben kleine Hilfe
- Verhandelt mit der Polizei (Wenn eure Strategie dies zulässt), spielt auf Zeit und macht immer wieder Druck. Wir wollen keine Straftaten begehen, aber lassen uns auch nicht ohne Konsequenz in unserem Recht beschneiden
- BEI ZUGRIFF der Polizei müssen sofort Ketten gebildet und Solidarität gezeigt werden! Es betrifft jeden, also zeigt das auch. Haltet jeden Fest, den ihr greifen könnt und lasst euch nicht kriminalisieren oder einschüchtern. Wir haben ein Grundrecht zu demonstrieren und werden davon selbst dann Gebrauch machen, wenn sie uns mit Schlägen drohen. FILMT wenn möglich Polizeigewalt und geht danach gemeinsam juristisch vor

11.5.7 Aktionsformen (Beispiele)

Folgend einige Ideen für Aktionsformen aufgelistet. Keine starren Vorgaben, sondern Anreize. Diskussionen über den Sinn führt ihr bitte bei euch. Auch eine Kombination ist natürlich möglich. Wenn euch eine Aktionsform nicht passt, verwendet sie einfach nicht.

Schwarzer Block
Der Schwarze Block (SB) dient der Durchsetzung von Demonstrationen und ermöglicht im Ziel eine anonyme Teilnahme.

Den SB macht vor allem das Bewusstsein aus, dass Freiheit ein langwieriger Kampf ist und der Weg dorthin nicht einfach umgangen werden kann. Der SB sollte als Kampf um die Straße und unsere Rechte verstanden werden, jeder Teilnehmer hält seinen Kopf für die anderen hin. Friedliche Lösungen sollten nicht ausgeklammert, sondern auch im SB angestrebt werden - solange sie in unserem Interesse sind und nicht unser Recht auf Demonstration beschnitten wird. **Der SB darf nicht asozial auftreten, sondern nur bestimmt.**

Bezeichnend für den SB ist ein einheitlich schwarzes Auftreten, wodurch einer extremen Repression entgegengewirkt werden soll. Der SB muss nicht immer ein gutes Bild abgeben, sondern soll

einen Sinn erfüllen. Dies müssen auch die anderen Gruppen immer beachten und respektieren.

Der SB wird in einen aktiven und einen passiven Block unterteilt. Weiteres unter der Durchführung auf Aktion

- Mögliche Ziele:

Demonstration ermöglichen
Recht auf Anonymität durchsetzen
Gefährliche Angriffe abwehren
Repressionen fokussieren und abwehren
Friedliche Demonstration ermöglichen, solange der Staat diese gewillt ist durchzusetzen. Sonst Durchsetzung dieser

- Mögliches Material (Besonderheiten):

Schwarze Klamotten zum Wechseln. Achtet darauf, keine auffälligen Symbole oder Farben zu tragen. Besprecht bitte, ob und wie ihr eine Vermummung zulassen wollt in eurer Gruppe. Diese macht im SB als Schutz vor Repressionen Sinn!
Schwarze Regenschirme
Schnipsel, Aufkleber u. Propagandamaterial (auf V.i.S.d.P. und Legalität achten, vorher absprechen!)
Faustis (Kleine Fahnen für die Faust), Fahnen (wenn Anreise in zivil kann dies ein Problem sein, ggf. versteckt ihr die Fahne und zieht diese erst später auf die Stange), Transparente zur späteren Blockbildung

- Mögliche An-/Abreise (Besonderheiten):

Mit Wechselkleidung in zivil oder als großer Pulk bereits im Block. Bei Letzterem erhöhte Repressionsgefahr vor der Aktion!
Regenschirme können bei Treffpunkten genutzt werden, falls ihr repressive Presse ausmacht oder offensichtlich beobachtet werdet
Schwarz gekleidete Menschen fallen besonders auf!

- Mögliches Verhalten bei der Aktion (Besonderheiten):

- Transparente werden, wie vorher geübt, ausgepackt und sofort an die Seiten und die Front gebracht. Werden Seitentransparente untersagt, sollte über ein Durchsetzen dieses Rechts nachgedacht werden. Friedlich aber bestimmt sollte der Eingriff in die Reihen verhindert werden, dazu zählt auch, dass keine verschiedenen Blöcke hintereinander gebildet werden. Dies macht nur bei bürgernahem Auftreten Sinn. Wenn schon, dann richtig, oder gar nicht
- Ein Block wird nicht mit Abständen gebildet, sondern durch die komplette Füllung jeder Lücke
- Während der Formierung drängt der SB nach vorne und versucht ein Blockieren des Zuges zu verhindern. Auch zuvor kann der SB schon Stellung beziehen und Druck machen. Wenn alle nur wahllos an einem Ort herumstehen, sieht die Polizei keinen Grund in einer Durchsetzung der Demonstration!
- Sollte es zu Streit innerhalb des Blocks kommen, immer wieder zur Ruhe animieren und respektieren, dass jeder seine Idee hat. Jedoch müssen manche Menschen auch erst „auf den richtigen Weg“ gebracht werden. Im Schwarzen Block hat niemand etwas verloren, der in

genau diesem Moment den Moralapostel spielen will. Es geht um Durchsetzung und Druck. Im Notfall muss der WORTFÜHRER eingreifen

- Dank einer guten Absprache kommt es selten zu Streit, öfter aber zu plötzlicher Entsolidarisierung. Hier wird plötzlich Pyrotechnik gezündet und da fliegen ein paar Flaschen und schon distanziert sich der halbe Block aus Angst vor Repression. Dies darf nicht passieren. Wir unterstellen jeder BG ein gewisses Ziel und vertrauen auch auf die Umsetzung, eine Diskussion kann es erst danach geben. In diesem Augenblick ist nichts schädlicher als Spaltung, denn dann kann der Staat sich Leute rauskrallen. Provokateure müssen unbedingt zu Recht gewiesen werden, sollte es sich eindeutig um eingeschleuste Personen handeln, müsst ihr gegen diese vorgehen! Duldet keine Kriminalisierung des Blocks und verhindert Randale und Eskalation!
- AKTIVER SCHWARZER BLOCK wird jener Teil bezeichnet, der vorne Druck macht und an den Seiten für Ruhe und Kraft sorgt. Der aktive SB verlässt sich auf den passiven, sodass wenn es z.B. nach Angriffen der Polizei zu Festnahmen kommt, Opfer sofort nach hinten gezogen und geschützt werden. Der aktive SB ist mithin der gefährlichste Teil, da dieser oft mit Pfefferspray und Schlagstöcken drangsaliert wird.
- PASSIVER SCHWARZER BLOCK ist der Teil, der den Block vorne „füttert“. Lücken müssen unbedingt gefüllt und verletzte Kameraden abtransportiert werden. Der passive SB nimmt auch ggf. Lasten (Rucksäcke, Material, ...) an sich, um vorne den Leuten eine bessere Dynamik zu ermöglichen. Bei Repressionen schließt der passive Block die Rückseite und verhindert ein Eindringen von hinten in die Demo.

Weiß-Hemden
Das typische Auftreten, z.b. beim TRAUERMARSCH BAD NENNDORF, wenn man sich volksnah zeigen möchte. Das weiße Hemd und die schwarze Hose, meist eine Zimmermannshose, vermitteln Ordnung und Disziplin. Zu Unrecht wird den Trägern dieser Uniformierung eine gewisse Weichheit unterstellt - sinnvoll aufgestellte, meist völkisch orientierte, Gruppen sind im Gegenteil sehr straff organisiert und durchaus durchsetzungsfähig.

- Mögliche Ziele

Trauermarsch oder Demonstration ordentliches Bild geben
Inhalte vermitteln
„das gute Gesicht“ unserer Bewegung zeigen

- Mögliches Material (Besonderheiten):

Ordentliche Kleidung
Zumeist keine Vermummung
Viele Fahnen, selten Transparente
Regenschirme können auch für diese BGs interessant sein!

- Mögliche An-/Abreise (Besonderheiten):

Meist mit Autos, da die „Uniform“ sehr schnell erkannt wird und Feinde sich besonders gerne solche Personen raussuchen

- Mögliches Verhalten bei der Aktion (Besonderheiten):

Reihenbildung, diszipliniert in gleicher Anzahl pro Reihe
Fahnen werden ordentlich getragen
Sollte die Demonstration blockiert werden und ein Schwarzer Block auf der Demo agieren, diesem

Vorrang lassen um Druck aufzubauen!
Trotz Angriffen von außen strickt den Weg weiter gehen und nicht beirren lassen

Nachhause-Schicker
Ja, auch so etwas kann man vorhaben. Kriminelle Antifaschisten attackieren immer wieder die friedlichen Demonstranten. Dem kann man vorher schon entgegenwirken, wenn einige Gruppen unterwegs sind, die die Antifa wieder nach Hause schicken. Es gilt die Gewalt gegen unsere Kameraden auf der Demo und die Übergriffe zu verhindern, in dem präventiv dafür gesorgt wird, dass die Kriminellen gar nicht erst anreisen können. Selbstverständlich geben wir keinerlei Anleitung zur gewalttätigen Auseinandersetzung, diese sucht ja schon die Antifa mit ihren Aufrufen zur Gewalt. Bestimmt aber zielsicher werden diese Menschen wieder in ihre Schranken gewiesen. Wieso wir auf die Idee kommen? **U.a. dieser Aufruf, gefunden in einer linken Zeitschrift und auf einer Netzseite, zeigt es. Linke ticken nicht ganz sauber und die Polizei schaut weg. Selbst handeln? Überlegt es euch. Wie? Müsst ihr wissen!**

Inglourious Basterds

- Es gibt Szenelinke, die uns abfällig als »Sportgruppe« bezeichnen. Aber das stimmt nicht. Was wir machen, hat nichts mit Sport oder gar sportlicher Fairness zu tun.**Im Gegenteil, wir greifen maskiert und ohne Vorwarnung aus dem Hinterhalt an. Allgemein wird so etwas als »unehrenhaft« oder als »feige« bezeichnet. Zugegeben, ein gewisser Pragmatismus ist uns zu eigen, aber im Unterschied zu Hooligans oder irgendwelchen Straßenschlägern arbeiten wir ergebnisorientiert.** Unser Ziel ist ganz simpel: Wir wollen den Nazis weh tun.

- Wichtig ist uns vor allem dabei, dass es die richtigen trifft, und nur die richtigen. Kollateralschäden nehmen wir nicht in Kauf. **Zumeist lauern wir einzelnen oder kleinen Gruppen von bekannten oder deutlich erkennbaren Neonazis auf. Wir folgen ihnen unauffällig und überwältigen sie dann in einem günstigen Moment. Alles muss dann schnell gehen. Wenn die Gegner weglaufen, um Hilfe schreien oder zurückschlagen, dann haben wir etwas falsch gemacht.** Manchmal nehmen wir ihnen dabei auch die Buttons ab oder reißen ihre Nazi-Shirts kaputt. Früher haben wir die einfach als Trophäen mitgenommen. Das machen wir nicht mehr, weil solche Beweisstücke für uns Serientäter gefährlich sein könnten.

- Der 13. Februar ist seit Jahren ein Pflichttermin für uns. Schon auf dem Weg nach Dresden treffen wir auf einer Autobahnraststätte eine Horde Dorfnazis. Es sind zu viele, um sie direkt anzugreifen. Also begnügen wir uns damit, heimlich die Reifen ihrer Autos zu zerstechen, und fahren dann weiter.

- Dresden ist an diesem Tag eigentlich nichts für notorische Leisetreter wie uns, sondern eher eine Spielwiese für autonome Hasskappen-Fetischisten, die, im Gegensatz zu uns, die offene Konfrontation mit den Bullen oder dem Nazimob suchen. Problematisch ist, dass sich Nazis und Linke nur noch schwer an der Kleidung unterscheiden lassen und man fast ausschließlich an große Gruppen gerät. Ob die Gruppe Halbvermummter, die einem da entgegenkommt, Antifas, Nazis oder gar Zivis sind, weiß man erst, wenn man sich direkt gegenüber steht. Wir begegnen mehrfach aggressiven Nazigruppen, die auf der Jagd nach Linken sind, uns aber nicht als Antifaschisten erkennen. Unser modus operandi funktioniert hier nicht, wir konzentrieren uns lieber darauf, Autos und Busse von Nazis zu beschädigen.

- Später fahren wir in eine ostdeutsche Kleinstadt. Am Bahnhof lauern wir mehrere Stunden vergebens auf Nazis, die aus Dresden zurückkommen. Unsere Geduld wird nach einer Weile mit einer zufällig vorbeikommenden Gestalt belohnt, die einen Pullover der Marke Consdaple trägt. Hierbei handelt es sich um Texilien, die von Nazis für Nazis gemacht werden und die

das Parteikürzel NSDAP mit dem englischen Wort »constable« verbinden. Uns ist klar, dass dem Bedürfnis, andere zu verletzen oder zu bestrafen, nichts Emanzipatorisches innewohnt. Was wir machen, wird als »politisch unbedeutend«, bestenfalls als »Gegenterror« kritisiert werden. Das wissen wir. Wir machen es trotzdem. Wenig später geht ein völlig überraschter Neonazi schwer angeschlagen zu Boden und verwandelt sich dort in ein wimmerndes Häuflein Elend. Ziel erreicht - wir fahren nach Hause.

Und jetzt zu uns. Unsere Agitation unterscheidet sich natürlich von der einer Demonstrations-Gruppe. Wir können hier nur kleine Anregungen geben.

- Mögliche Ziele:

Anreise von illegalen Blockierern und Straftätern verhindern
Druck auf die linke Szene ausüben

- Mögliches Material:

Keine politischen Sachen
Eure Ausstattung bestimmt sich dadurch, wieweit ihr gehen wollt!

- Mögliche Agitation:

Gezielt Anreise mit möglichen Blockierern unserer legalen Aktion und diese vorher blockieren oder wieder nach Hause schicken
Achtet auf eure Umgebung. Zivilpolizei
Polizei
Antifa schon da?
Macht Treffpunkte der Antifa im Netz aus, vielleicht trefft ihr ja zufällig schon auf dem Weg zu dem Treffpunkt einen netten Bekannten? Am Treffpunkt solltet ihr natürlich nicht ankommen, außer ihr seid natürlich darauf ausgerichtet.
Lieber 1-2 Stunden nichts getan und abgewartet, beobachtet und Fotos geschossen, als zu weit in Gefahr gebracht.
An der Anreise hindern = Autotreffpunkte finden? Denkt euch was aus

Anti-Repressions-Team

- Anti-Antifa:
Auch auf der Demonstration selbst könnt ihr viel gegen die kriminellen Roten machen. Oder ihr begebt euch gar nicht erst auf die Demo, sondern beobachtet von außen! Anti-Antifa Arbeit ist Aufklärungsarbeit. Wer kennt wen, wer geht nach der Blockade oder Aktion wohin? Auch bei normalen Demos der Antifa, eigentlich gerade da, ist Anti-Antifa Arbeit am effektivsten. Dort seht ihr wer aktiv ist, wer wen kennt und könnt vielleicht auch noch rausfinden wo manche Aktivisten wohnen.

- Anti-Repression:
Lasst niemanden alleine etwas machen, sondern bildet auch hier eine BG um den Fotografen zu schützen. Auch hier müsst ihr ggf. etwas anders vorgehen und einteilen, die Aufgaben beziehen sich nun natürlich auf andere Gebiete.

- Mögliche Ziele
Aufklärung über kriminelle Strukturen
Schutz eigener Struktur
Aufklärung über Polizeigewalt

- Mögliches Material (Besonderheiten):
Fotoapparat, Videokamera
Presseausweis wenn vorhanden
Wenn ihr nicht auf einer Demo seid: Einen Fahrer, der euch schnell weg bringen kann
- Mögliche An-/Abreise (Besonderheiten):
Ihr fahrt als normale Demoteilnehmer? Dann schaut oben und überlegt euch, ob ihr im schwarzen Block auftreten wollt. Solltet ihr vorne dabei sein, schützt eure Kamera gut
Als eigenständige, unauffällige Gruppe unterwegs? Agiert vorsichtig.

- Mögliches Verhalten bei der Aktion (Besonderheiten):
Bei Polizeigewalt sofort die Kamera nach vorne, ggf außerhalb des Blocks um genaue Repression zu filmen
Kameraden über Repression und Gesetze aufklären

- Blockade
Kriminelle zu blockieren, die immer wieder Übergriffe vollziehen, sollte für jeden aufrechten Menschen Normalität sein. Sei es das sabotieren der Anreise oder das aktive Blockieren auf einer Demo-Route - es gibt viele Möglichkeiten und wir können aufgrund der Repression hier keine weiteren Hinweise geben. Sucht euch die Aktionsformen der Gegenseite raus und passt diese an, auch Tiertransporter oder den Bau von Moscheen, linken Zentren etc. kann man so verhindern / behindern.

- Weitere Aktionsformen
Weitere Aktionsformen gibt es viele. Bitte recherchiert und überlegt euch auch Methoden, die vielleicht nicht exakt auf eine der oberen passen.

11.5.8 Übung macht den Meister

Das volle Programm mit viel Trara müsst ihr nicht jedes Mal machen. Auch wirkt es vielleicht alles aufwändiger als es tatsächlich ist, im Endeffekt muss einmal klar sein, wie der Ablauf ist - dann klappt die Rollenverteilung und das Besprechen bei der nächsten Aktion auch wesentlich schneller. Trotzdem kann und sollte man gerade bei neuen Aktionsformen und etwas gefährlicheren Manövern ein paar Übungen durchführen.

Training auf dem Feld
Training kann eine gute Ergänzung neben dem einfachen Besprechen der Aktion sein. Hierzu sucht ihr euch einen Ort aus, der abgelegen von der Stadt ist.

Trainiert mit zwei BGs (10-20 Leute machen Sinn), wie ihr auf Eingriffe der Polizei reagiert und wie ihr euch organisiert.

Vergebt die Rollen und einen Moderator, der das Spektakel von außen betrachtet und dirigiert.

Bildet zum Beispiel eine angreifende und eine Demo-Gruppe. Oder übt das Ketten bilden bei Eingriffen der Polizei, das behindern der repressiven Presse, ... Beobachtet euer Verhalten redet danach drüber! Wertet aus und besprecht mögliche Verbesserungen.

11.5.9 Nach der Aktion

Nach der Aktion müsst ihr euch zusammensetzen und mindestens folgende Fragen besprechen:

Wie lief die Aktion?

WAS haben wir falsch gemacht?

Wo waren unsere Fehler? Seid ehrlich und offen!

MÜSSEN wir Stellung abgeben, weil irgendetwas besonders aufgefallen ist?

Fertigt eine interne Stellungnahme an und kritisiert auch euer eigenes Verhalten, lasst euch aber nicht auf eine einseitige und ergebnislose Diskussion von Hetzern und Spaltern ein

WIE können wir unser Vorgehen perfektionieren?

Besser vorbereiten?

GAB ES grobe Verstöße gegen die vorher besprochenen Grenzen und Regeln und wieso? Juristische Nachbearbeitung

Jede Nacharbeitung erfordert auch, an die nächste Aktion zu denken. Wenn wir uns immer wieder alles gefallen lassen, dürfen wir uns nicht beschweren.

Kam es zu Ausschreitungen, ist mit Ermittlungen zu rechnen - hierfür müsst ihr euch unbedingt mit anderen Gruppen absprechen und Gedankenprotokolle schreiben! (Vorlage siehe Artikel zum Thema „Outing“).

Kam es zu Angriffen auf Kameraden ebenfalls absprechen! Bildet einen Ermittlungsausschuss, wenn dieser nicht vorhanden ist. Nur so können die vielen Anzeigen gegen euch und auch diese gegen Polizisten sortiert werden. Sammelt zusammen alle Beweise, die ihr gegen den repressiven Apparat nutzen könnt.

Wurde euer Recht beschnitte? Schreibt gemeinsam möglichst ausführliche Klagen, lasst euch nicht in euren Rechten beschneiden.

Gab es Verhaftungen, Durchsuchungen, ... ? Reagiert.

Einer für alles
Viele Anwälte, die mit unserer Sache sympathisieren können gleich mehrere Kameraden vertreten und bei vielen Anliegen kurz und knapp helfen.

Normale Anwälte sind auch selten einem großen Kundenstamm abgeneigt, also kümmert euch rechtzeitig um einen Schutz. Schaut auch, was eure Rechtschutzversicherung abdeckt.

11.5.10 Schlusswort

Diese Broschüre soll eine erste Hilfe für alle sein, die Interesse an Bezugsgruppen haben. Es ist eine erste Ausarbeitung und sicher werden einige, die sonst nie auf die Idee gekommen wären etwas Produktives zur Bewegung von sich aus beizutragen, ihren Senf dazu abgeben. Davon lassen wir uns aber nicht blenden. Wir sind stolz darauf, dass wir es geschafft haben, alle Ideen und Aspekte die uns eingefallen sind, zu Blatt zu bringen. Wenn ihr weitere Anregungen habt oder Erfahrungen sowie berechtigte Einwände, schreibt uns an akbildung@0x300.com . Auch wenn es oft genug schon gesagt wurde: Das sind alles Ideen. Nehmt sie auch so hin. Kombiniert alles nach Belieben und entdeckt eure eigenen Strategien - wir wollten unsere mitteilen, damit auch andere etwas davon haben. Wer immer nur stänkert aber selbst nichts gebacken bekommt, kann uns gestohlen bleiben. Wir wünschen sehr, sehr, sehr viel Spaß und Erfolg bei der Umsetzung, aber vor allem bei den

Übungen!

Unser politisches Streben ist kein Zuckerschlecken, da ist jedes Lachen und jede Freude Gold wert. Gönnt euch diese schönen Momente! Und damit meinen wir nicht die Momente, bei denen wir da sitzen und nichts tun. Viel geiler sind Tage, an denen wir total fertig von Aktionen kommen und wieder wissen, weshalb wir diesen Weg gehen. Gegen die Repression hilft nur Solidarität und Humor. Eine Menge. Von beidem. Abschließend noch einige Hinweise: Wir arbeiten ehrenamtlich und geben sehr viel Zeit, Nerven und auch Geld dafür aus, anderen den Weg zu erleichtern und ihnen zu helfen. **Bitte respektiert das und spendet ruhig auch kleine Beträge, Büromaterial, Bücher, ... An den Arbeitskreis könnt ihr euch gerne wenden, dieser vermittelt Spenden dann an Lesekreise, Aktionsgruppen und und und. Zehn Euro tun nicht weh, schließlich musstet ihr auch nicht das Risiko, die Arbeit und das Herzblut investieren. Unsere Leute bleiben am Ende auf den Klagen sitzen um euch zu schulen! Also, bringt euch ein und gebt denen, die bei der Verbreitung helfen, ein bisschen was. Wir sind kein Verein und keine Tafel!**

Zum Thema Sicherheit wurde ein gesonderter Leitfaden herausgegeben. Unter dem Titel Verhalten gegenüber Polizei und Justiz wird eine Broschüre bereitgestellt, die im Notfall sehr nützlich sein kann. Auch zum Thema Verhalten bei einem feindlichen „Outing“ gibt es bereits ein Heft. Besorgt euch diese und verbreitet, verbreitet, verbreitet. Bildung soll man nicht sammeln, sondern allen mitteilen - sonst bringt auch unsere ganze Arbeit nix!

Es grüßen euch eure üblichen Verdächtigen,

Arbeitskreis Bildung & Sicherheit

12 Allgemeine Hinweise

12.1 Anti-Antifa - Kleines Einmaleins für die Recherche

Die Anti-Antifa ist eine direkte Antwort auf die konsequent feindlichen Aktivitäten von Antifa-Gruppen. Die Anti-Antifa beschreibt sich selbst als Informationssammelstelle zur „Feindaufklärung“, die persönliche Daten politischer Gegner sammelt und veröffentlicht, sowie deren Aktionen und Veranstaltungen dokumentiert. Diese Vorgehensweise wurde von der sog. „Outing“-Praxis vieler Antifa-Gruppierungen übernommen.

Die größte öffentliche Aufmerksamkeit erhielt die Anti-Antifa, als 1993 in einer Publikation mit dem Namen Der Einblick Personendaten von Linksextremisten, Journalisten und Politikern aus der gesamten Bundesrepublik veröffentlicht wurden. Dieser Artikel soll dir helfen, wenn du Hinweise oder Tipps brauchst, um bei der Anti-Antifa Recherche weiterzukommen.

12.1.1 Recherche als Grundlage politischer Arbeit

Recherche für die politische Arbeit umfasst mehr als die Untersuchung des linkskriminellen Spektrums. Wenn eine politische Gruppe ihre Entscheidung nicht alleine auf einer Gefühlsbasis treffen will, muss sie sich auf die Suche nach Fakten begeben, sie muss Recherche betreiben.

Fakten sind wichtig, um die Realität genau beschreiben zu können. Die Realität muss erfasst und analysiert werden, um auf Grundlage von Fakten in der Lage zu sein, politische Schlussfolgerungen für die eigenen Aktivitäten zu ziehen.

- Recherche ist nach Fakten graben. Fakten auszugraben ist ebenso hart wie nach Kohle zu graben. Es bedeutet, sie aus dem Untergrund emporzuschleudern, nach ihnen zu bohren, sie

abzumeißeln, sie wegzuschaufeln und einzuladen, sie an die Oberfläche zu holen, abzuwiegen und an die Öffentlichkeit zu bringen als Brennstoff - für Feuer und Wärme. Fakten bescheren ein Feuer, das nicht gelöscht werden kann.

- Um Kohle zu fördern, braucht es Bergarbeiter. Um Fakten an die Oberfläche zu fördern, braucht es ebenfalls Bergarbeiter - Faktenbergarbeiter. Die Besitzer (der Minen - d.Ü.) wissen, was sie wollen und bekommen es. Die Arbeiter wissen nicht was sie wollen und das bekommen sie zu spüren.

Recherche ist aber auch mehr, als Fakten zu finden. Wenn die Fakten „ein Feuer“ bescherensollen, müsst ihr auch darüber nachdenken, wie ihr die Ergebnisse der Recherchen für eure Arbeit benutzt. Ihr müsst euch überlegen, zu welchem Zeitpunkt und gegenüber welchen Menschen ihr die Fakten präsentieren wollt.
Das Thema der Recherchen muss das Ergebnis einer politischen Diskussion sein. Die Erfahrungen zeigen, dass Leute, die Recherche betreiben, sich leicht verzetteln, wenn ihre Arbeit nicht eingebunden ist in eine politische Arbeit. Nur aus der politischen Diskussion ergeben sich die Fragen: „Was wollen wir erreichen, wie viel können wir machen, was müssen wir dafür wissen?“ Die Beantwortung dieser Fragen grenzt das Gebiet der Recherche ein.

Bestimmt gemeinsam, welche Informationen ihr braucht, um handeln zu können!
Grenzt das Thema und den Umfang eurer Recherche ein!
Bestimmt als Gruppe das Ziel der Recherche!
Passt auf, dass ihr vor Fakten nicht das Ziel eurer Gruppe aus den Augen verliert!

12.1.2 Recherche gegen Linkskriminelle

Recherche gegen Links hat das Ziel herauszufinden

wie stark der Gegner ist,
wo er neue Leute rekrutiert,
was seine aktuellen Pläne von Strategie und Taktik sind,
welche konkrete und welche zukünftige Gefahr von ihm ausgeht,
wo seine Aktions- und Argumentationsschwerpunkte liegen,
wo er auf Zustimmung und wo er auf Ablehnung stößt.

Die Beantwortung dieser Fragen ermöglicht die Bestimmung wirksamer Gegenaktionen.

Jede Gruppe sollte sich in dem Bereich, in dem sie handelt, besser auskennen als ihr Gegner. Dies schützt sie selbst und andere vor bösen Überraschungen oder Niederlagen. Das gilt auch für die politische Öffentlichkeitsarbeit. Das Ziel ist, den Widerstand gegen die Aktivitäten der Linkskriminellen zu fördern.

Die Aufklärung von bisher Verborgenem kann Leute wütend machen und oft den Beweis erbringen, der gebraucht wird, um öffentliche Empörung herzustellen. Daher werden bei der Recherche in erster Linie Fakten gesammelt, die die eigene Position stärken. Das bedeutet aber nicht, dass Fakten so lange verdreht werden bis sie in die eigene Position passen. Durch das Präsentieren gesicherter und nachprüfbarer Fakten entsteht Vertrauen - dagegen entsteht durch das Präsentieren von Lügen und Unwahrheiten Misstrauen. Gefährlich wird es, wenn falsche Zitate die Runde machen. Wenn sich solch ein „Beweis“ in Luft auflöst, kann das neben dem politischen Schaden auch rechtliche Folgen haben.

Wenn ihr zu einem Thema recherchiert, also Informationen sammelt und auswertet, werdet ihr manchmal feststellen, dass sich auch euer eigener Blick auf die Angelegenheit verändert. Ihr erkennet den Kern der Sache vielleicht deutlicher und könnt eure eigenen Forderungen besser und klarer

darstellen. Wenn ihr während einer Recherche versuchet, die Stärken und Schwächen des Gegners herauszufinden, heißt das auch, die eigene Situation im Verlauf der Recherche zu analysieren.

Wenn ihr vorher Verborgenes herausfindet oder wenn ihr feststellt, dass es außer euch auch noch andere gibt, die die Augen offen halten und Kritik äußern, dann zeigt das auch, wo ihr mit eurer Arbeit vorher gestanden habt und wo ihr hinkommt. Es wird klarer werden, welchen Einfluss der Gegner hat und was ihr selbst könnt.

Die Recherche verändert eure Blickwinkel, ob ihr es merkt oder abstreitet. Deshalb ist es wichtig, die Aktivisten, die Recherche machen, nicht alleine arbeiten zu lassen. Genauso wie die Gruppe über das Ziel der Recherche bestimmt, müssen die Ergebnisse mit allen ausgewertet werden. Das stärkt das Selbstvertrauen der Gruppe und ihrer Mitglieder und verhindert, dass Recherche-Leute „abheben“. Wenn ihr wisst, warum eine Sache wichtig ist, werdet ihr mit euren Mitteln immer besser umgehen, als wenn ihr unsicher seid.

Bei der Recherche gegen Linksextremisten gibt es Informationen, die vertraulich behandelt werden müssen. Vertraulich deshalb, weil sie Personen gefährden könnten. Informationen können nicht nur diejenigen gefährden, die eure Gegner sind. Auch die, die diese Information besitzen oder sie weitergegeben haben, können gefährdet sein. Achtet deshalb darauf, dass ihr die Vertraulichkeit mancher Informationen beachtet. Solche „Geheimnisse“ können gerade bei der Recherche gegen Links großen Spaß machen. Der Spaß mancher Geheimnisse besteht leider nur darin, das Geheimnis zu lüften. Besprecht gemeinsam, wie ihr damit umgehen wollt. Wenn ihr am Kneipentisch Geschichten erzählt bekommt, weil die Leute wissen, sie erzählen es „der Anti-Antifa“, fragt nach, ob die Infos vertraulich sind oder nicht. Und überlegt trotzdem gut, ob ihr diese Informationen gebrauchen könnt oder nicht. Recherche gegen Linksextremisten hat nur wenige Freunde.

Im gegensatz zu der Antifa-Recherche, die von Justiz, Polikern und der Presse angespornt und belohnt wird, kämpfen nationale Aktivisten gegen ihre Repressionen. Das Linkskriminelle Weltnetzportal Indymedia wurde mit einem Deutschen Medienpreis ausgezeichnet während die vom NW-Berlin erstellte Chronik Linkskrimineller Aktivitäten Kriminalisiert und als „geheime Hass-Liste“ der Berliner Nazisdiffamiert wurde. Inzwischen wurde ein Rechtshilfegesuch der brd Regierung an die USA gestellt, da die Seiten dort gehostet waren. Dies hatte das Ergebnis, das beide Weltnetzseiten abgeschaltet wurden und die Nutzerdaten von den Amerikanischen Behörden herausgegeben worden. Gegen die Initiatoren werden zur Zeit gerichtliche Verfahren geführt.

Als nationale Aktivisten die Anti-Antifa-Arbeit betreiben müsst ihr also über die Maße konspirativ Arbeiten! Wenn ihr die Ergebnisse eurer Arbeit ins Weltnetz stellen wollt darf dies ausschließlich mit Hilfe von Anonymisierungstools passieren.

12.1.3 Quellen der Recherche

Presseauswertung
Die normalen Tageszeitungen berichten teilweise über Linksextremen Aktivismus. Der Umfang der Berichterstattung richtet sich nach dem Markt- bzw. Sensationswert der Meldung. Das bedeutet, dass die Berichterstattung genauso abrupt zu Ende sein kann, wie sie anfängt. Trotzdem sind Presseartikel wichtige Bausteine für die Recherche. Das Ausschneiden, Auswerten und Archivieren gehört daher auch zur Anti-Antifa-Arbeit. Zeitungen, Broschüren, Infotelefone und Fanzines der Linken geben wichtige Einblicke in ihre Aktivitäten und Pläne. Da die meisten Publikationen nicht am Kiosk zu haben sind, müssen sie bestellt werden. Wenn ihr etwas bestellt, denkt daran, dass die Linkskriminellen in ihren Karteien nach eventuellen „Nazis“ suchen und auch gelegentlich zu Besuchen vorbeischauen. Elektronische Medien

Viele Zeitschriften und Tageszeitungen können inzwischen über das Weltnetz eingesehen werden. Natürlich haben auch Linkskriminelle PProfilein sozialen Netzwerken wie Facebook und können

für die Recherche wichtig sein.

Die Linkskriminellen sind auch schon lange mit eigenen Weltnetzseiten im Netz. In Portalen wie Indymedia, wo offen zur Gewalt gegen alles was nicht in ihr Weltbild passt aufgerufen wird, werden Bekennerschreiben oder Ankündigungen regelmäßig von den Moderatoren gelöscht. Hier gilt es schneller als die Moderatoren zu sein und diese Antikel am besten per Screenshot (Druck S-Abf Taste) archivieren und auswerten. Zu dem Thema Sicherheit im Weltnetz kann - und muss - natürlich ziemlich viel gesagt werden. Wer sich im Weltnetz bewegt, hinterlässt Spuren. Wer das Weltnetz als Quelle stark nutzt, muss sich hier schützen.

Im Netz kann man sich aber auch sehr gut als Antifaschist bewegen, Foren und Chat-Räume besuchen und darüber an interne Informationen oder Gerüchte kommen. Und wer ein paar Hilfsmittel kennt, kann die Spuren, die Antifas hinterlassen, selber nutzen, um sie zu enttarnen. Hier ist es aber besonders wichtig, nicht jeden Hinweis als Tatsache weiter zu verbreiten! Gerade die Anonymität im Netz sorgt dafür, dass ihr nur sehr schwer nachprüfen könnt, ob etwas wahr ist bzw. wer eine Aussage tatsächlich gemacht hat. Beobachtung

Die Beobachtung von Aktivitäten der Linkskriminellen ist eine wichtige Grundlage für euch als politische Gruppe. Ihr könnt herauszufinden und darstellen, wie hoch der Organisationsgrad der Antifas ist, welche Pläne sie verfolgen und wer mit wem zusammenarbeitet etc.

Ihr könnt z.B. Flugblattaktionen beobachten, um herauszufinden, wie die Antifas solche Aktionen organisiert. Genauso interessant sind ihre Veranstaltungen oder internen Treffen oder ihre Demonstrationen und auch Blockaden. Die Beobachtung von Antifa-Aktivitäten ist nicht ohne Risiko.

Ihr solltet euch angemessen kleiden und unauffällig verhalten. Auf jeden Fall solltet ihr Linksextremisten und deren Aktionen nicht alleine beobachten. Sichert euch immer ab und organisiert einen Schutz - macht nichts alleine!

Zu Dokumentationszwecken könnt ihr fotografieren, filmen, Flugblätter einsammeln oder Reden aufnehmen. Autonummern geben euch einen Überblick, ob zu einem Treffen auch überregional mobilisiert wurde.

Ein besonderer Fall sind Gerichtsverhandlungen. Wenn „wichtige“ Personen vor dem Richter stehen, solltet ihr auf jeden Fall den Besuch der Verhandlung organisieren. Die meisten Prozesse sind öffentlich und werden durch Aushang bekannt gegeben. Die Presse erhält über telefonische Anfrage Auskunft bei der Justizpressestelle.

Dokumentation und Öffentlichkeitsarbeit
Ein oft vernachlässigter Bereich ist die Dokumentation von antideutschen und antifaschistischen Übergriffen und Aktivitäten. Gerade wenn ihr in einem bestimmten Stadtteil arbeitet, können Zeugenaussagen viele Informationen hergeben, die sonst verborgen bleiben. Dazu müsst ihr Kontakt mit den Betroffenen aufnehmen oder eventuellen Augenzeugen ausfindig machen.

Die ganzen schlauen Infos nutzen nichts, wenn sie unter eurem Bett verstauben. Ihr solltet euch grundsätzlich überlegen, wie ihr die Öffentlichkeit informieren wollt. Veranstaltungen, Flugblätter, Broschüren oder Zeitschriften sind Mittel, die ihr selbst gestalten könnt.

Filme, Videos und Fotos
Wenn ihr auf der Suche nach Filmen oder Fernsehbeiträgen von bestimmten Anlässen seid, wird es schon komplizierter. Eigene Mitschnitte, am besten regelmäßig, werden euch nicht erspart bleiben. Es gibt allerdings Archive, die auch Fernsehsendungen aufnehmen.

Die öffentlich-rechtlichen Sender sind da noch mal was Besonderes. Diese haben einen vom Gesetzgeber bestimmten Bildungsauftrag mitbekommen und riesige Archive, bei denen ihr auch nachfragen könnt. Sie sammeln nicht nur Film- oder Radiobeiträge, sondern haben meist auch Presseauschnitte und Fotos zu wichtigen Themen, Personen, Organisationen. Grundsätzlich ist die Nutzung kostenlos. Ruft einfach an und fragt nach.

Anders ist es bei den privaten Sendern, die so etwas nicht kennen. Fernsehbeiträge unterliegen dem Urheberrecht. So ist es oftmals einfacher Manuskripte von interessanten Sendungen zu bekommen als komplette Mitschnitte. Einfach anrufen oder Brief schicken mit frankiertem Rückumschlag. Das genaue Datum hilft natürlich auch. Manche Skripte findet ihr inzwischen auch im Weltnetz.

Öffentliche Register
Damit sind das Grundbuchamt, das Handelsregister und das Vereinsregister gemeint. Öffentliche Register sind Angelegenheiten der jeweiligen Gemeinden. Sie sind prinzipiell für jederman zugänglich und einsehbar. Dort findet ihr Angaben darüber, wem was seit wann gehört, bzw. wer welchen Verein betreibt.

Bei allen drei Registern handelt es sich um öffentliche Einrichtungen, deren Zweck die Erteilung von Auskünften ist. Am häufigsten werden die Einträge von Behörden (Polizei, Justiz) oder bestimmten Berufsgruppen (Rechtsanwälte, Notare, Journalisten) genutzt. Es ist also überhaupt nichts dabei, wenn ihr dort auftaucht. Im Prinzip jedenfalls. Die Erfahrung zeigt, dass die Erteilung von Auskünften von Ort zu Ort und von Register zu Register sehr unterschiedlich gehandhabt wird. Manche Mitarbeiter entwickeln z.B. ein reges Interesse für euch.

Im Vereinsregister sind alle Vereine eingetragen, die ein „e.V.“ tragen. Das Register wird normalerweise im zuständigen Amtsgericht geführt. Die Zuständigkeit richtet sich nach dem Sitz des Vereins, der nicht unbedingt identisch mit Postanschriften, Büroadressen oder ähnlichem sein muss. Im Register wird eine Akte des Vereins und eine Registerkarte geführt. Die Akte enthält u.a. das Gründungsprotokoll, Protokolle von Mitgliederversammlungen, Schriftwechsel zwischen dem Verein und dem Gericht, die Satzung und so weiter. Auf der Registerkarte sind die entscheidenden Angaben über Sitz, Vorstand und Adresse angegeben. Auch jeder Vorstandswechsel wird hier vermerkt.

12.2 Selbstverständlich Wahlbeobachter - Aber wie?

Eine parlamentarische demokratische Wahl ist öffentlich. Die entsprechenden Regelungen, die Wahlbeobachtungen bzw. die Öffentlichkeit der Wahl erlauben, finden sich in der BRD meist in den Landesverfassungen, zusätzlich in den entsprechenden Landeswahlgesetzen sowie im Grundgesetz. Jeder hat das Recht, eine Wahl zu beobachten, unabhängig von Alter, Geschlecht, Nationalität, Wohnsitz, Fachwissen oder Zugehörigkeit zu Organisationen. Wie wichtig eine Wahlbeobachtung ist zeigt dieser Bericht auf dem Portal: www.altermedia-deutschland.info[5]

Eine „vollständige“ Wahlbeobachtung, wie sie zum Beispiel vom ODIHR (Office for Democratic Institutions and Human Rights, einer OSZE-Organisation) durchgeführt wird, dauert mehrere Monate und beginnt lange vor dem Wahltermin.

Diese Beobachtung im Vorfeld ist wichtig, allerdings nur mit viel Fachwissen und finanziellen Mitteln möglich. Realistisch ist für einen politischen Aktivisten daher die Beschränkung der Wahlbeobachtung auf den Wahlsonntag.

[5] vom Netz genommen - geht besser auf www.einprozent.de

Die Beobachtungen müssen selbstverständlich so ablaufen, dass die Wahl in keinem Fall gestört wird. Das Verhalten des Wahlbeobachters ist also stets höflich und ruhig, am besten „unsichtbar“.

12.2.1 Vorbereitung der Wahlbeobachtung

Siehst du in und an dem Gebäude, in dem sich der Wahlraum befindet, oder unmittelbar vor dem Zugang zum Gebäude Wahlwerbung, mache den Wahlvorstand darauf aufmerksam und verlange die sofortige Beseitigung. Wahlwerbung in und vor Wahllokalen ist nach den geltenden Wahlgesetzen verboten.

Drohe notfalls mit Einspruch gegen die Wahl, gemäß dem Wahlprüfungsgesetz. Der Einspruch muss binnen einer Frist von zwei Monaten nach dem Wahltag beim Wahlleiter eingehen. Verboten ist „jede Beeinflussung der Wähler durch Wort, Ton, Schrift oder Bild“. Das heißt, dass auch Kommentare nach dem Motto, das Kreuz an der richtigen Stelle zu machen usw. nicht erlaubt sind. Schon gar nicht aus den Reihen des Wahlvorstandes.

Die Adressen der Wahllokale, die besucht werden sollen, sind vorab zu ermitteln. Es empfiehlt sich das Anfahren der Wahllokale bereits am Vorabend. Notiert werden sollte ebenfalls die Nummer des zentralen Wahlleiters sowie die Adresse des zentralen Wahlbüros.

Praktische Dinge zum Mitnehmen sind:

Mobiltelefon
Digitalkamera - Fotografieren ist zwar nicht verboten, es sollte aber während der Öffnungszeiten des Wahllokals vorab erfragt werden, ob Fotografieren erwünscht ist.

Wähler und Wahlhelfer haben dabei stets das Recht am eigenen Bild und sollten keinesfalls ungefragt fotografiert werden

Stadtplan
Adresse/Telefonnummer des Wahlleiters
Notizblock und Stift
Ordentliche Klamotten

Das Tragen von T-Hemden mit politischen Aufdrucken kann als Beeinflussung gelten und muss unterbleiben

Gehe rechtzeitig ins Wahllokal, damit du bei der Auszählung ab 18 Uhr von Anfang an dabei bist. Sollte man dich bei der Auszählung nicht dabei haben wollen, berufe dich auf die entsprechende Wahlordnung. In der Bundeswahlordnung heißt es dazu: „Während der Ermittlung und Feststellung des Wahlergebnisses hat jede Person zum Wahlraum Zutritt, so weit das ohne Störung des Wahlgeschäfts möglich ist.“ Drohe notfalls mit Einspruch gegen die Wahl. Mache dir genaue Notizen!

Wähler dürfen innerhalb des Wahllokals nicht angesprochen werden. Sollte es Interesse an Gesprächen mit Wählern geben, so muss der „Bannkreis“, in dem eine Beeinflussung der Wähler verboten ist, beachtet werden.

Es besteht keine Altersbegrenzung für Wahlbeobachter, auch unter 18 Jahren darfst du anwesend sein. Weiterhin gibt es keine zeitliche Begrenzung der Anwesenheit und du musst nicht vor Ort wohnen. Als Wahlbeobachter kannst du also in jedes beliebige Wahllokal gehen.

12.2.2 Beobachtung der „Auszählung“

Generell ist es wichtig, eventuelle Beobachtungen möglichst genau zu notieren. Aus diesem Grund sollte immer Zettel und Stift zum sofortigen schriftlichen Festhalten bereitliegen. Jeweils sollten dazu Zeit, Ort und genaue Beobachtung festgehalten werden. Vermutungen sind dabei nicht wichtig, nur Fakten und persönliche, eigene Beobachtungen sind sinnvoll.

Achte besonders darauf, dass niemand Stimmzettel verschwinden lässt. Der Zählvorgang beginnt damit, dass alle Stimmzettel aus den Wahlurnen auf einen Tisch geschüttet werden. Dann wird zunächst die Gesamtzahl der abgegeben Stimmen festgestellt - diese unbedingt notieren.

Während der Auszählung ist darauf zu achten, dass gültige Stimmen nicht in ungültige verwandelt werden.

Zweifelsfrei ungültig sind Stimmzettel:

auf denen mehr als ein Wahlvorschlag angekreuzt ist
die Zusätze oder Vorbehalte enthalten
die schwer beschädigt (etwa durchgerissen) sind

Das gilt aber nur, wenn sich die Stimmzettel vor der Auszählung in einem solchen Zustand befinden - nicht, wenn sie von einem Auszählenden beschmiert oder beschädigt werden

Gültig sind Stimmzettel auch:

wenn nur ein Kandidat oder nur eine Partei angekreuzt ist, also nur die Erst- oder die Zweitstimme abgegeben wurde wenn kein Kreuz, sondern ein anderes Symbol die gewollte Partei kennzeichnet

Es kommt darauf an, dass der Wählerwille zweifelsfrei zu erkennen ist. Das kann gem. § 34 Bundeswahlgesetz durch ein auf „Stimmzettel gesetztes Kreuz oder auf andere Weise“ geschehen, Ein Punkt oder ein „Ja“ in oder neben dem zum Ankreuzen vorgesehenen Kreis kann als gültige Stimmabgabe angesehen werden.

Solche Fälle werden unter den Auszählenden diskutiert. Du darfst an diesen Beratungen zwar nicht teilnehmen, dokumentiere aber mit genauer Uhrzeit jede zweifelhafte Entscheidung.

Eine kurze Warnung, dass hier ein Anlass für eine Wahlanfechtung oder gar eine Strafanzeige wegen Wahlfälschung, § 107a StGB, vorläge, kann angebracht sein.

Dokumentiert werden sollte, wer welche Schritte durchführt und wie die organisatorischen Vorgaben für die Meldung des Ergebnisses an das zentrale Wahlbüro sind. Notiere alle Zwischenergebnisse und vor allem auch das Endergebnis, das der Wahlvorstand dann telefonisch an den Landeswahlleiter gibt. Das können die Parteien dann mit dem offiziellen Resultat vergleichen.

Wenn es möglich ist, sollte auch die zentrale Ergebnisermittlung (meist im Rathaus) beobachtet werden.

12.2.3 Probleme?

Solange du dich freundlich und zurückhaltend verhälst, sollte es zu keinen Problemen kommen.

Wenn die anwesenden Wahlhelfer die Beobachtung verbieten wollen, solltest du freundlich auf grundlegende Rechte hinweisen und die Wahlhelfer zur Rücksprache mit dem zentralen Wahlleiter

anhalten. Wenn dieser Bitte nicht entsprochen wird, solltest du selbst den zentralen Wahlleiter anrufen und dir bestätigen lassen, dass eine Wahlbeobachtung tatsächlich nicht erwünscht ist. Sollte dies passieren, muss es dringend protokolliert werden, denn dies kann ein schwerwiegender Wahlfehler sein.

12.2.4 Nach der Wahl

Dass die Wahlauszählungen beobachtet werden, ist von der Wirkung her nicht zu unterschätzen. Beobachter aus vergangenen Jahren berichten, dass sie bei JEDER Auszählung, an der sie teilnahmen, Stimmen für die NPD herausholen konnten, die sich beispielsweise fälschlich auf dem Stapel der ungültigen Stimmen wiederfanden. Wahlbeobachtung ist Wahlkampf bis zur letzten Minute und ebenso wichtig, wie Flugblätter, Infotische und Plakate.

Jede Stimme für Deutschland zählt - deshalb darf Wahlfälschern keine Chance gegeben werden! Wenn du Unregelmäßigkeiten findest, melde den betreffenden Parteien deine Ergebnisse und Erfahrungen. Sie werden die Ereignisse nach der Wahl auswerten und veröffentlichen. Bei Wahlmängeln werden sie Einsprüche gegen die Wahl und ggf. Strafanzeigen stellen.

12.3 Wie erstellt man ein Flugblatt?

Öffentlichkeitsarbeit bedeutet, dein Anliegen öffentlich zu machen. Flugblätter (Flyer) bieten dir die Möglichkeit, auch die Bürger mit Informationen zu versorgen, die keine Zeit oder keine Lust haben, mit dir auf der Straße zu reden. Ein Flyer kann naturgemäss mehr Informationen transportieren als ein Plakat. Dennoch werden die meisten Anliegen so komplex sein, dass nicht alles auf einen Flyer paßt, so dass du dich auf das wichtigste beschränken musst. Zudem muss der Flyer das Interesse des Lesers wecken. Das geht nicht mit einer Bleiwüste. Der Leser muss in die Lage versetzt werden, wichtige Kernaussagen auf einen Blick zu erfassen. Beispielsweise ist ein Bild, eine Zeichnung oder ein Logo als Blickfang und als Aufhänger fürs Weiterlesen geeignet. Bietet dein Anliegen einen Facettenreichtum, der mit vielen Informationen verbunden ist, so ist diese Informationsflut eigentlich nur mittels Aufschaltung einer Weltnetzseite zu bewältigen. Der Flyer weist dann auf die Weltnetzseite als umfassende Informationsquelle hin. Heutzutage verfügen die meisten Haushalte über einen Zugang zum Weltnetz. Auch ältere Bürger, die deinen Flyer lesen und keinen eigenen Computer haben, können Freunde und Bekannte bitten, für sie im Weltnetz zu schauen und etwas auszudrucken.

12.3.1 Gestaltung eines Flugblattes - A I D A

AIDA bedeutet Attention (Aufmerksamkeit), Interesting (Interesse wecken), Desire (Wünsche wecken), Action (Der Leser soll Aktivitäten entfalten). Das sind die Stufen, die sich in den Gedanken des Lesers abspielen sollen, damit der Flyer ein höchstes Maß an Effektivität erzeugt. Schaue dir Flyer und Direktwerbungen an, die in deinem Briefkasten landen. Besuche Weltnetzseiten anderer Bürgerinitiativen. Lade deren Flyer herunten und vergleichen Sie: Welche Aufmachung spricht Dich besonders an, welche findest du weniger gelungen?

Aufmerksamkeit und Interesse werden durch schlagzeilenartige Kurz-Infos erzeugt. Bsp. „Keine Asylantenheime in Wohngebieten“. Stellen sie dann den Sachverhalt, also einige Fakten, und ggf. auch mögliche Folgen, dar. Z.B. dass der bevorstehende Bau eines Asylantenheimes den Wert der anliegenden Häuserreihe stark schrumpfen lässt, dass die kriminalität steigen wird etc. Bei Großprojekten stellt sich zudem immer die Frage, wer denn konkret einen Nutzen davon hat. Auch so eine Frage kann im Flyer aufgeworfen werden.

Der Flyer soll beim Leser zumindest den Wunsch erwecken, dass Ihre Initiative Erfolg haben wird. Das kann sich bereits aus der Sachverhaltsdarstellung ergeben - es gibt Sachverhalte, die ein

normalempfindender Bürger einfach ablehnen muss. Du kannst im Flyer auch ausdrücklich formulieren (als eine Art Positiv-Liste), wie schön die Zukunft sein könnte, wenn die Initiative Erfolg hat.

Aktion beim Leser - das bedeutet, dass der Flyer etwas beim Leser bewirken soll. Im Falle eines Flyers einer Bürgerinitiative könnte das sein:

Werden Sie Mitglied
Spenden Sie an die Bürgerinitiative
Schreiben Sie an den Oberbürgermeister und an die Ratsmitglieder, die Adressen bekommen Sie bei uns
Empfehlen Sie uns in Ihrem Freundes- und Bekanntenkreis weiter
Kommen Sie zur Demo am ... um ...
Besuchen Sie Vortrag den der Bürgerinitiative zu diesem Thema am ... um ...
Kommen Sie mal an einem Info-Stände oder bei einem unserer Treffen vorbei. Wir treffen uns jeden Samstag abend um ... in ...

Leite z.B. mit Worten über wie:

Sie können die Zukunft mitgestalten. Helfen Sie uns, indem Sie ...

12.3.2 Wichtig: V.i.S.d.P.

Flugblätter, Plakate, Aufkleber... - alle Druckwerke sind verpflichtet ein korrektes Impressum zu tragen. Festgeschrieben wird das in den Landespressegesetzen, die sich meist stark ähneln. Es bietet sich an, diese Angaben kleingedruckt am Ende oder in die Fußzeile des Flyers aufzunehmen. Ein Impressum besteht meist aus folgenden Teilen:

V.i.S.d.P.: steht für Verantwortlich im Sinne des Presserechts
Name: Vor- und Nachname - Anfangsbuchstaben sind nur erlaubt, falls eine gerichtliche Ladung erfolgen kann
Anschrift: eure komplette Anschrift, ein Postfach soll nicht erlaubt sein, es liegt aber keine Gerichtsentscheidung vor
Anschrift des Druckers: Im Normalfall bleibt es beim Eigendruck im Selbstverlag - E.i.S.

Das könnte dann in etwa so aussehen:

Max Mustermann, Beispielstraße 22, 30519 Schilda - E.i.S.

Wer hingegen Druckwerke mit falschem oder fehlendem Impressum herstellt begeht eine Ordnungswidrigkeit, die mit einer Geldstrafe belegt werden kann. **Das Verteilen oder Verkleben von Flugblättern oder Plakaten mit falschem oder fehlendem Impressum ist erlaubt! Lediglich der Verleger begeht eine Ordnungswidrigkeit.**

12.3.3 Drucken eines Flugblattes

Da gibt es mehrere Möglichkeiten: Zu Hause mit dem eigenen Laserdrucker, im Copy-Shop, in einer örtlichen Druckerei oder bei einer Druckerei im Weltnetz.

Zu Hause
Vorteil ist die Flexibilität: Du kannst oft und spontan kleine Serien drucken und diese auch geringfügig variieren. Nachteil: Je nach Drucker und verwendeten Papier ist es nötig, dass du während des Druckens dabei bist und aufpasst, dass kein Papierstau entsteht und das Papier den Drucker ordentlich verlässt. Es könnte sich wellen oder knicken. Du musst DIN-A4-Blätter mittels einer

Papierscheidemaschine auf DIN-A5 bringen. Das kostet zusätzliche Zeit. Du musst Papier und Toner günstig einkaufen und sich einen Vorrat anlegen. Das können für 20.000 DIN-A5-Flyer schnell mehrere Hundert Euro sein.

Es empfiehlt sich, zwei DIN-A5-Flyer auf eine DIN-A4-Seite zu drucken. Am einfachsten ist es, die Flyer in der Textverarbeitung auf DIN-A4-Größe zu erstellen und dann verkleinert - auf DIN-A5 - je zwei Flyer auf eine DIN-A4-Seite zu drucken. Dazu stellst du entweder den Druckertreiber (die meisten können das heutzutage) oder das Druck-Fenster deiner Textverarbeitung (z.B. ab winword 2000 / openoffice) entsprechend ein. Die Funktionen heißen sinngemäß: „Mehrere Seiten auf ein Blatt drucken“ und bieten idR. die Auswahl, ob 2,4 oder 8 Seiten verkleinert auf ein Blatt gedruckt werden sollen. Experimentiere ein bißchen damit, bevor du eine größere Anzahl Flyer druckst.

Kaufe einen Laserdrucker mit niedrigen Druckkosten. Tintenstrahldrucker machen keinen Sinn; sie sind langsam und der Ausdruck ist teuer und die Tinte neigt zum Verwischen, wenn das Blatt feucht wird. Der Drucker sollte mit preisgünstigen Fremdkartuschen, also Tonerkartuschen von Drittanbietern, betrieben werden können. Erkundige dich im Freundes- und Bekanntenkreis nach geeigneten Druckern. Bsp: Laserdrucker Brother HL-2030 (120 Euro), Tonerkassette für 2.500 Seiten (Original 64 Euro, Fremdhersteller im Weltnetz 33 Euro zuzüglich Versand). Tipp zur Abnutzung der Bildtrommel: Drucke stets viele Seiten (10, 20, oder mehr) nacheinander, so arbeitet die Bildtrommel bei gleichförmiger hoher Temperatur und erreicht eine lange Lebensdauer

Anders wäre es, wenn nur hin und wieder mal ein Brief gedruckt wird. Wir empfehlen, für den Flugblattdrucker neben genügend Tonerkassetten auch eine Bildtrommel in Reserve zu halten. Preisgünstige Anbieter für Toner und anderes Druckerzubehör findest du mittels Suchmaschine im Weltnetz. Falls dein Druckertreiber über eine Einstellung TTonersparmodusverfügt, probiere diese aus. In der Regel ist die Druckqualität auch beim Tonersparmodus sehr gut und die Druckkosten pro Seite sinken dadurch etwas. Copy-Shop oder örtliche Druckerei

Vorteil ist die Beratung. Bei größeren Auflagen (um 1.000 Exemplare) kostet es 4ct pro DIN-A4-Seite. Bei doppelseitigem Druck 8 ct pro DIN-A4-Blatt. Gut ist die Beratung und dass du nach der ersten Probekopie schon die Qualität beurteilen kannst und das Gerät vom Copy-Shop-Personal ggf. anders einstellen lassen kannst.

Internet-Druckerei
Du musst die Druckseite (bei doppelseitigen Flyern: Vor- und Rückseite) als pdf-Datei übermitteln. Problematisch kann die erstellte PDF-Datei sein, wenn dazu kostenlose pdf-Konvertierungsprogramme aus dem Weltnetz verwendet werden, die sich als Druckertreiber installieren. Eventuell ist die Qualität der Grafiken unzureichend. Probiere eine Weltnetzdruckerei erst einmal mit einer kleineren menge von Flyern aus, damit du nicht soviel Geld in den Sand gesetzt hast, wenn das Ergebnis nicht überzeugt. Wir habe gute Erfahrungen bei der Erstellung von pdf-Dateien mit dem aktuellen openoffice 2.x gemacht. Druckkosten können sehr niedrig sein: Bei einer Auflage von 5.000, Vierfarb-Doppelseitigdruck und 135-g-Papier 2 ct pro DIN-A5-Flyer.

Einige Weltnetzdruckereien verlangen, dass die eingesendete pdf-Datei nicht eine genormte Papiergröße (DIN-A5 / DIN-A4 etc.) hat, sondern an jedem Rand ein paar Millimeter überstand hat. Das ist nötig für die Produktion. Stelle bei openoffice statt des zu druckenden Zielformates (z.B. „DIN-A5“ für Ihren DIN-A5-Flyer) eine benutzerdefinierte Blattgröße ein, die den von der Druckerei geforderten Überstand zuschlägt.

Bsp: Die Druckerei möchte zu jeder Seite 2 mm zusätzlichen Rand haben. Also stelle das benutzerdefinierte Papierformat auf eine 4mm größere Blatthöhe und eine 4 mm größere Blattbreite ein. Bsp. bei DIN-A5 (14,8 cm * 21 cm): 15,2 cm * 21,4 cm.

12.3.4 Verteilen eines Flugblattes

In Einfamilienhausgebieten mit Hinterliegergrundstücken kannst du etwa 100 Flyer pro Stunde absetzen. In Mehrfamilienhaus-Wohngebieten sind es viel (bis zu zehn mal) mehr. Falls die Briefkästen nicht von außen zugänglich sind, kann man klingeln bis sich jemand meldet. Rufe kurz „Postwurfsendung", in der Regel wird dir dann geöffnet.

An Info-Ständen kannst du ebenfalls Flyer absetzen. Du kannst den Bürgern den Flyer wortlos anbieten oder einfach sagen „Guten tag, es geht um ... ". Jeder hat da seinen Stil. Das Aussehen und das Auftreten des Aktivisten spielen eine herausragende Rolle bei der Frage, wieviele Bürger Flyer entgegennehmen. Und: Wenn einer einen Flyer annimmt, nehmen die ihm unmittelbar folgenden Passanten mit einer höheren Wahrscheinlichkeit ebenfalls einen Flyer ab als wenn du ein- oder zwei Abfuhren bekommen hast. Probiere es aus.

Du kannst örtliche Einzelhändler fragen, ob sie deinen Flyer an deren Tür hängen können oder ob er einen Stapel Flyer auf dem Tresen neben der Kasse auslegt. Auf diese Weise werden vielfach Informationen verbreitet, die für die örtliche Gemeinschaft interessant sind. Manche Discounter verfügen über ein „Schwarzes Brett" für derartige Informationen.

12.4 Wie erstellt man ein Transparent?

Transparente haben die Aufgabe, auf Demos, bei Protestaktionen oder Infoständen eine Nachricht zu vermitteln, aufzuklären oder das Anliegen des Protestes zu vermitteln. Gerade wenn die laute Geräuschkulisse der Demo oder andere ungünstige Umstände verhindern, dass interessierte Passanten den Grund des Protestes verstehen, nehmen Transparente eine extrem wichtige Rolle ein. Deshalb ist nichts unangenehmer für die Protestierenden, als unleserliche, zerknitterte Transpis, die gerade gegen Ende der Demo von den erschöpften Trägern nur noch auf „Halbmast" gehalten werden.

Wir möchten euch Möglichkeiten aufzeigen, einfach und kostengünstig praktische und funktionale Transpis selbst zu basteln!

12.4.1 Erfolgsrezepte und Todsünden

Das Transparent ...

sollte eine einfache Botschaft klar vermitteln
sollte optisch etwas hermachen
muss optisch schnell und klar erfassbar sein
sollte wetterfest sein
sollte reisefest sein
sollte bequem zu halten und nicht all zu schwer sein

Gar nicht geht ...

uneindeutige Aussagen, oder „Insider"-Nachrichten, die nur mit Hintergrundwissen zu verstehen sind
zu viel Schrift
schiefe Schrift die im Laufe der Zeile immer kleiner wird
Rechtschreibfehler
verlaufene Schrift durch Regen
Transpis, die schwer zu transportieren sind
Transpis, die kompliziert zu halten sind, oder leicht Falten/Wellen schlagen und so schwer zu lesen sind

12.4.2 Das regenfeste und sehr haltbare Bilder-Transparent

Transpis sollen Aussagen vermitteln. Gemäß dem Spruch „Bilder sagen mehr als tausend Worte“ macht es bei manchen Themen Sinn in ein Transparent zu investieren, das sowohl ein einprägsames Bild enthält, aber auch wetterfest und leicht zu transportieren ist. Ihr braucht

Poster oder Bilddatei von deinem gewünschten Motiv (optimalerweise ein oder zwei Poster im Format DIN-A2)
Einen Copyshop in deiner Nähe, der Poster laminieren kann; oder durchsichtige Klebefolie
Durchsichtiges Klebeband, am Besten schön breit
Schere
gegebenenfalls Holz-Besenstiele
gegebenenfalls dicke Pappe

Schritt 1: Das Motiv
Vielleicht habt ihr ein Transpimotiv im Sinn, z.B. zum Thema „Volkstod“. Ihr könnt nun entweder eines der Poster verwenden, die von zahlreichen Aktivisten zur Verfügung gestellt werden, euch eine Fotodatei aus dem Weltnetz besorgen oder ein neues Motiv an euerm Computer erstellen.

Schritt 2: Das Laminieren
Ihr solltet euer Transpimotiv nun fertig haben. Geht zu einem Copyshop, der Poster in der Größe DIN-A 3 bzw. DIN-A 2 laminieren kann (d.h. in Plastik einschweißen) und lass dein Poster laminieren. Falls ihr eure Bilddatei am Computer erstellt habt, könnt ihr eure Datei auch im Copyshop ausdrucken lassen. (Kosten ca. 5-7 Euro). Bei der Bilddatei solltet ihr darauf achten, dass die ursprüngliche Bildgröße und das Format passend sind. Falls euer ursprüngliches Bild zu klein war, wird es unscharf, wenn ihr es auf eine zu große Fläche drucken lasst. Mit Format ist das Verhältnis der Seiten zueinander gemeint. Das heißt, ihr solltet darauf achten, dass ihr die euch zur Verfügung stehenden Fläche möglichst vollständig nutzt. Ansonsten habt ihr viel weißen Rand um das eigentliches Transparent.

Ein Transparent kann auch aus 2 zusammengeklebten Teilen bestehen. Eine große Fläche kann sich auch aus mehreren kleineren Flächen zusammensetzen. Dafür musst du dein Bild für den Druck durch die Mitte in zwei (oder mehrere) Teile teilen. Diese fügst du nachher wieder zusammen. Alternativ zum Laminieren im Geschäft könnt ihr Klebefolie verwenden. Das macht ihr aber am Besten zu zweit. Schneidet euch zuerst ein etwas größeres Stück Klebefolie aus, als ihr für die Posterfläche benötigt und legt es mit der nicht klebenden Seite nach unten auf den Boden. Jeder von euch nimmt sich jetzt ein Ende eures Posters und von einer Seite zur anderen wird das Poster langsam und vorsichtig auf die Klebefolie gedrückt. Passt auf, dass sich keine Luftblasen oder Falten bilden. Hier kann es hilfreich sein, das Poster mit einer harten Kante (z.B. Lineal oder feste Bürste) auf die Folie zu drücken. Danach schneidet ihr die Ecken ein und faltet und klebt den überstehenden Folienrand auf die Rückseite eures Posters. Dasselbe macht ihr dann mit der Rückseite eures Posters und schon ist das Transpi vor Wind und Wetter perfekt geschützt.

Schritt 3: Zusammenbau und Montage der Besenstiele
Die Poster (je nach Anzahl und Größe) müssen nun mit dem durchsichtigen Klebeband aneinander geklebt werden. Ihr könnt euer Poster auch mittels Klebeband oder Schnur am Besenstiel befestigen. Falls die Schnurvariante bevorzugt wird, solltet ihr das Bild professionell laminieren lassen, da beim Laminat die Plastikschicht dicker ist und der sehr punktuellen Beanspruchung durch die Schnur besser standhält. Andererseits lässt sich das Transparent dadurch schwerer zusammenrollen.
In dieser Hinsicht ist das Klebefolientranspi vorteilhafter, da es wesentlich flexibler ist und sich für den Transport leichter um den Besenstiel wickeln lässt, ohne sich nachher ständig von selbst wieder aufzurollen. Der obere Besenstiel schaut im Optimalfall etwas über die Seiten hinaus, da das Transparent so leichter zu tragen ist.

Anwendungsmöglichkeit Schilder
Natürlich könnt ihr auf diese Art auch Schilder basteln. Dazu legt ihr das Poster/den Ausdruck auf ein Stück dicke und stabile Pappe. Die Pappe sollte genau so groß sein wie das Poster. Das erreicht ihr am Besten, indem ihr entweder euer Poster vermesst und euch dann ein entsprechendes Stück Pappe mit einem Teppichmesser zurechtschneidet oder das Poster auf die Pappe tapt und vorsichtig mit dem Teppichmesser die Außenkanten abfahrt. Bei der zweiten Methode muss das Klebeband erneuert werden, wenn es mit der Pappe abgeschnitten wurde. Bei der ersten Methode fahrt ihr am Besten an einem geraden Gegenstand (z.B. Lineal) entlang, damit die Kante exakt gerade wird. Dann wird das Poster mit viel breitem Klebeband an die Pappe geklebt. Achtet darauf, dass das Klebeband sehr glatt und sauber verklebt ist, damit möglichst kein Spalt auf der Forder- oder Rückseite frei bleibt. Dadurch wird das Schild wasserdicht und auch etwas stabiler. Ihr könnt noch mit Klebeband einen Besenstiel auf die Rückseite tapen, damit das Schild höher gehalten werden kann. Ansonsten kann man es auch einfach so in den Händen halten.

Vorteile
Das Transpi kann jederzeit auseinander und zusammengebastelt oder restauriert werden. Es ist extrem leicht zu tragen und vermittelt Botschaften sehr eindrücklich. Für längere Transporte kann es (meistens) einfach zusammengerollt werden. Bilder und grafisch aufwendige Designs sind auch schon mit geringem Kostenaufwand realisierbar.

12.4.3 Das klassische Bettlaken-Transparent

Was wird benötigt[6]?

- Ein schwarzes Bettlaken (diese sind in der Regel fester/dicker als weiße Bettlaken und nehmen Farbe besser auf; Schmutz ist auf ihnen weniger sichtbar und die Signalwirkung stärker)
- Wasserfeste, gut deckende Stofffarbe (auch Stoffacrylfarbe genannt), Acrylfarben, Lacksprühfarbe oder Wandfarbe und Pinsel (Achtung, keinen Tierhaarpinsel kaufen!)
- Haarspray
- Ein Transpimotiv
- Tafel
- dicker, schwarzer Edding

Bei besonderen Techniken braucht ihr außerdem gegebenenfalls

- 2 Besenstiele
- Schnur
- Nadel und Faden
- Cuttermesser/Skalpell
- dünne, feste Pappe und Kleber
- Beamer / Tageslichtprojektor mit bedruckbarer Folie
- Computer und Drucker

[6]Bilder zur Veranschaulichung auf s-f-n.org

Der Stoff sollte etwas fester sein und natürlich nicht all zu teuer. Betttücher haben sich hier als recht geeignet erwiesen. Ihr könnt bei Krankenhäusern, Altenheimen usw. anfragen ob sie euch aussortiertes Bettzeug zur Verfügung stellen. (Oder schaut auf Flohmärkten, in Secondhand-Läden oder Läden der Arbeiterwohlfahrt) aber auch in verschiedenen Geschäften könnt ihr Bettlaken preisgünstig erstehen. Da habt ihr dann auch mehr Auswahl, was die Farbe betrifft. Auch Meterware aus Stoffgeschäften, Stoffabteilung von Kaufhäusern, IKEA etc. ist geeignet.

Die Farbe, die auf den Stoff kommt, sollte deckfähig, knick-, wasser- und witterungsbeständig sein. Hierfür geeignete und leicht erhältliche Farben sind Wandfarbe, Acrylfarben, Stofffarben (auch Stoffacrylfarben genannt) oder Lacksprühfarben. Ihr findet sie in Baumärkten, Bastelläden, Billigläden usw. Wandfarbe sollte gut mit Wasser verdünnt werden.

Schritt 1: Das Motiv
Überlegt euch einen kurzen, klaren Spruch, der sich auf einem Transpi angemessen wiedergeben lässt z.B. „Nationalen Sozialismus Erkämpfen“, oder „Stoppt den Volkstod“ usw. Wichtig ist dabei, dass das Transparent nicht überladen wird. Also passt die Spruchlänge der Stofffläche an (oder anders herum). Beachtet auch, dass euer Transpi nicht durch zu viel Text schwer leserlich wird. Auch Zeichnungen und Symbole können das Transparent optisch aufwerten. Bevor ihr weiter macht, solltet ihr euch ziemlich genau darüber im Klaren sein, wie euer Transparent am Ende aussehen soll. Am Besten ihr skizziert eure Vorstellungen erst einmal. Falls ihr mehrere Aktivisten seid, werden anhand von Skizzen oft erst die verschiedenen Vorstellungen deutlich und vergessen könnt ihr euer Motiv dadurch auch nicht (klingt lustig, kommt aber des öfteren vor).

Schritt 2: Vorbereitungen
Am Anfang muss der Stoff gut vorbereitet werden. Er sollte nicht all zu verknittert oder dreckig sein. Je sauberer und glatter (evtl. bügeln) ein Stoff ausgelegt ist, desto besser nimmt er die Farbe auf. Bei fabrikneuen Stoffen empfiehlt es sich, diese vorher zu waschen, da Stärke in den Fasern sein könnte, was die Farbe schlechter haften lässt. Also möglichst vorher ohne Weichspüler waschen und jegliche Falten rausbügeln. Den Stoff dann auf dem Boden oder besser auf einem großem Tisch ausbreiten. Im Optimalfall spannt ihr den Stoff etwas, indem ihr an den Enden zieht und ihn dann mit Schraubzwingen fixiert. Das muss aber nicht sein. Unbedingt notwendig ist allerdings, genügend Zeitungspapier unterzulegen, ansonsten habt ihr das Transparent nachher als Durchschlag auf Tisch oder Boden.

Schritt 3: Motiv/Spruch vormalen
So jetzt kommt die Skizze wieder zum Einsatz. Nehmt die Kreide und malt zunächst (mit einem großen Lineal) sehr fein die Linien vor, auf die ihr später die Buchstaben zeichnen wollt. So vermeidet ihr schiefe Schrift. Malt danach die Buchstaben ebenfalls mit Kreide vor. So erkennt ihr, ob ihr die Größe der Buchstaben richtig eingeschätzt habt und ob irgendwo ein Rechtschreibfehler drinsteckt. Kreide lässt sich leicht ausklopfen, abbürsten oder mit einem befeuchteten Schwamm sofort abwischen. Um Transparente zu verschönern oder einfach leeren Platz zu füllen werden oft Bilder oder Symbole verwendet. Dazu aber später mehr.
Schritt 4: Farbauswahl und Buchstaben/Motiv malen
Überlegt euch spätestens jetzt, welche Worte ihr in welcher Farbe malen wollt. Wichtige Worte könnten z.B. die Signalfarben Rot oder Orange haben, Zwischenworte in Weiß. Im Optimalfall habt ihr das aber bereits mittels der Skizze geklärt. Nehmt euch kleine bis mittelgroße und starre Pinsel (ca. 1 cm breit), stell die Farbe auf einer Unterlage bereit und dann kann es losgehen. Beim Nachmalen entwickelt jeder Mensch mit der Zeit seine eigene Technik. Grundsätzlich gilt, ihr solltet eine Richtung einhalten, also beispielsweise in Leserichtung (von oben links nach unten rechts). Passt auf eure Hände auf und fasst nicht in die Farbe! Ansonsten ist alles erlaubt, was gut aussieht. Lasst die Farbe trocknen und malt gegebenenfalls noch 1-2 mal nach, bis die Farbe starke Deckkraft hat. Dann sorgfältig trocknen lassen. Kleinere Patzer könnt ihr bei schwarzem Stoff mit schwarzem Edding ausbessern, wellige Kanten korrigieren und Farbklekse verschwinden lassen. Einfach drübermalen wenn alles getrocknet ist.

Schritt 5: Farbe haltbar machen
Sprüht die aufgetragene und gut getrocknete Farbe mehrmals gründlich mit Haarspray ein. Achtet darauf, dass ihr die Dose nicht zu nah an die Schrift haltet und dass alles zwischen den Sprühgängen gut trocknet. Dadurch wird die Farbe gummiartig und reißt und bröckelt nicht.

Schritt 6: Ränder stärken
An den Außenkanten deines Transpis liegt der glatt abgeschnittene Stoff frei. Hier kann der Stoff unschön ausfransen oder einreißen. Da beides nicht sehr gut aussieht und die Lebensdauer des Transpis verkürzt, ist es sinnvoll die Ränder zu säumen. Mit Hand oder Nähmaschine, egal. Klappt den Soff an den Außenkanten ungefähr 1 cm um und fixiert ihn dort mit Steckadeln / Sicherheitsnadeln / Tape oder was sonst noch geeignet ist. Mit farblich zum Stoff passendem Faden näht ihr den Saum sauber auf den Stoff. Am Anfang und am Ende eurer Naht müsst ihr den Faden stabilisieren, damit die Naht nicht wieder aufgeht. Dazu näht ihr am Besten 2-3 mal vor und zurück. Dadurch könnt ihr den Faden leicht mit sich selbst verknoten. Mit einem 3-4 fachen Konten zum Schluss das Fadenende fixieren.

Schritt 7: Montage
Bei der Montage von Transparenten gibt es verschiedene Systeme. Größtenteils wird an diesem Punkt nicht mehr weiter gearbeitet und so wird das Transpi einfach am Stoff festgehalten, oder mit Tape an anderen Gegenständen befestigt. Praktischer und einfacher zu tragen ist das Transpi jedoch, wenn es mittels zweier Holzstangen stabilisiert wird. Durch 2 waagerechte am Stoff befestigte Besenstiele kann z.B. eine Einzelner Aktivist ein 2 Meter langes Transpi problemlos alleine halten. Spezielle Montagesysteme können also je nach Einsatzgebiet sinnvoll sein.

Wie bei Transpiart Nr. 1 wird nun das Bettlaken an die Besenstiele geknüpft. Vertikale Holzgriffe sorgen dafür, dass das Transparent relativ kräftesparend hochgehalten werden kann. Waagerechte Stangen sorgen dafür, dass weniger Träger benötigt werden und das Transparent gerader gehalten wird. Falls ihr Stangen einarbeiten wollt, stecht Löcher in den Stoff und verknüpft ihn mittels Packetschnur mit dem Besenstiel.

Noch perfekter und absolut stabil gelingt das Transpi, wenn du an den entsprechenden Seiten Tunnelhalterungen einnähst, d.h. den Rand so umnähst, dass ein Schlauch entsteht, in den eine Stange gesteckt werden kann. Das Transparent lässt sich dann problemlos einrollen und transportieren, ist leicht zu tragen und wirft kaum Falten. Wenn die Holzstangen herausgezogen sind, lassen sich Stofftransparente auf beachtlich kleinen Raum lagern und transportieren.

Schritt 8: ggf. Restauration
Wenn nach intensiven Gebrauch und Transport die Farbe spröde oder rissig wird, einfach die betroffenen Stellen noch einmal nachmalen, wieder mit Haarspray besprühen, fertig. Bei gerissenem Stoff könnt ihr versuchen, die Risse zu flicken. Aber bevor ihr ein total entstelltes Transpi verwendet, ist es wohl besser, ein neues zu malen. Entscheiden müsst ihr das selbst.

12.4.4 Schablonentechnik

Eine weitere Technik, Text auf ein Transparent zu bringen, ist die Schablonentechnik. Dabei werden einfach die Umrisse der Schablonen (z.B. von Buchstaben) mit Bleistift oder Kreide auf den Stoff aufgetragen und danach mit Farbe nachgemalt. Wenn mehrere Transparente geplant sind, oder es realistisch ist, dass weitere folgen werden, ist es sinnvoll das gesamte Alphabet in Kleinbuchstauben als Schablone zu erstellen. Alle Schablonen, die nach dem gleichem Schema erstellt wurden, könnt ihr dann in eine Mappe packen und darauf genau beschriften, welche Schriftart / Schriftgröße / besondere Einstellungen oder Bezugsflächen (dazu später mehr) verwendet wurde. So könnt ihr später defekte Schablonen problemlos wieder nachbauen.

Schritt 1: Die Schriftart
Ihr solltet euch erst einmal darüber klar werden, wie groß die Schrift nachher auf dem Transparent sein und wie sie wirken soll. Hier ist es hilfreich, einzelne Buchstaben auszudrucken und auf den Stoff zu legen, damit ihr euch ein genaueres Bild vom Größenverhältnis (Stofffläche / Buchstabengröße) machen könnt. Die Größe des Ausdrucks entspricht der Größe der Schrift auf dem Transparent. Experimentiert einfach einmal herum und probiert verschiedene Schriftarten, Schriftgrößen und Einstellungen, wie etwa fett, aus. Prinzipiell sind alle Schriftarten für die Schablonentechnik geeignet, aber unterschiedlich schwer umzusetzen. Wenn die Schrift extrem verschnörkelt ist, wird das Herstellen der Schablone und auch später das Ausmalen der Buchstaben unter Umständen langwierig und mühsam. Trotzdem, alles ist machbar! Die Einstellung fett ist grundsätzlich für Transparente recht gut geeignet, da die Schrift dadurch lesbarer und auffallender wird.

Schritt 2: Die Schablone basteln
Wenn ihr euch über die Schrift im Klaren seid, geht es an die Herstellung der Schablonen. Diese bestehen aus fester dünner Pappe (DIN-A4 Notizblock- oder Kalenderrücken, Müslischachteln usw.). Wichtig ist nur, dass eine gerade Kante vorhanden ist. Bei Schreibblockrücken ist diese sowieso vorhanden. Bei Müslischachteln müsst ihr euch mit Teppichmesser/Skalpell und Lineal eine Kante zurechtschneiden. Die Buchstaben druckt ihr wie gewünscht aus und klebt sie auf die Pappe. Hierbei darauf achten, dass die obere Kante eures Computerausdruckes mit der geraden Kante auf der Pappe übereinstimmt. Diese Kante ist dann euere Bezugskante. Sie bewirkt, dass euer Schriftzug nachher schön gerade ist. Geklebt werden sollte vorzugsweise mit Papierklebestift, notfalls klappt es mit Klebestreifen aber genau so. Danach werden die Buchstaben mit Teppichmesser oder Skalpell aus der Pappe geschnitten.

Beachtet dabei, dass sowohl das Herausgeschnittene (also z.B. der ausgeschnittene Buchstabe), als auch die Pappe, aus der der Buchstabe herausgeschnitten (Negativ-Form) wurde, als Schablonen verwendbar sind.

Ohne die herausgeschnitten Stücke („Inseln“) könnt ihr bei Buchstaben wie P, B, A oder O die Inseln nicht aufzeichnen, und ohne das restliche Pappstück wird die Schrift schnell schief. Also möglichst darauf achten, dass beide Teile unversehrt bleiben. Mit einem Skalpell arbeitet es sich angenehmer als mit einem Teppichmesser, zudem wird der Schnitt noch genauer. Bei geraden Linien könnt ihr ein Lineal anlegen und mit dem Schneidewerkzeug daran entlang fahren. Dadurch werden Kanten schön gerade und es geht nebenbei auch noch schneller. Die Bezugskante unbedingt mit einem Pfeil markieren, so dass ihr sie auch nach längerer Zeit noch erkennt. So, jetzt sind die Schablonen fertig.

Schritt 3: Das Auftragen
Auch hier malt ihr mit Kreide und einem großem Lineal zuerst eine gerade Linie. An dieser Linie wird die Bezugskante eurer Schablonen angelegt und die entsprechenden Buchstaben mit Bleistift nachgemalt. Falls der Buchstabe eine Insel enthält, müsst ihr den ausgeschnitten Buchstaben auf den Umriss legen, um die Insel einzeichnen zu können. Wenn ihr alles eingezeichnet habt, lest es nochmals aus einigen Metern Distanz auf Rechtschreib- und Grammatikfehler durch. Wenn ihr euch bei einem Wort nicht sicher seid, schlagt es nach, denn über Rechtschreibfehler auf Transpis machen Passanten sich gerne lustig und nehmen dann eure Aussage nicht ernst. Wenn ihr dann auch noch mit der Flächeneinteilung zufrieden seid, könnt ihr, wie oben schon beschrieben, die Buchstaben ausmalen, trocknen lassen, mit Edding ausbessern und mit Haarspray fixieren.

12.4.5 Bilder und Symbole auf Transparenten

Um Transparente zu verschönern oder einfach leeren Platz zu füllen, werden oft Bilder oder Symbole verwendet. Um diese in guter Qualität auf das Transparent zu bringen kann man sich entweder der Beamermethode bedienen oder mittels Stencils arbeiten. Es ist aber auch durchaus möglich Bilder mit Kreide vorzumalen und später einfach nachzuzeichnen. Für gute Ergebnisse braucht es

hier aber etwas Übung und/oder Talent.

Der Tageslichtprojektor/Beamertrick
Wer die technischen Möglichkeiten hat, kann auch ganz professionell mit einem Tageslichtprojektor oder Beamer Transparente erstellen. Das Transpimotiv zuerst am Computer erstellen und dann mittels Beamer auf das Transpi projezieren. Das Verfahren ist auch mittels Tageslichtprojektor und bedruckbarer Folien praktizierbar. Das Transparent wird dazu an die belichtete Wandfläche gehängt. Wichtig ist, dass der Stoff keine Falten wirft und wirklich fest an der Wand hängt. Ihr könnt ihn entweder mit Reißzwecken anpinnen oder mit gut haftendem Tape ankleben. Hier gilt, lieber zu viel als zu wenig. Die Konturen der Grafik werden dann mit Bleistift nachgefahren. Ihr arbeitet am exaktesten, wenn ihr auf Augenhöhe malt. Da habt ihr den Stift am Besten im Blick und eure Arme ermüden nicht so schnell. Falls ihr euch vermalt, könnt ihr mit einem weichen Radiergummi ausbessern. Beim Radieren das Transpi nicht von der Wand reißen!

Wenn alles aufgezeichnet ist, und ihr mit dem Ergebnis zufrieden seid, könnt ihr das Transparent von der Wand nehmen und die Formen wie schon zuvor beschrieben ausmalen.

12.5 Wie erstellt man eine Sprühschablone?

Weil die Mal- oder besser Sprühkünste vieler eher bescheiden sind, wollen wir uns mit der Herstellung einer Sprühschablone beschäftigen. Dabei setzen wir die Anforderung, dass die Schablone keinen Einschränkungen bezüglich der Form oder Größe ausgesetzt ist. Auch sollte die Schablone wiederverwertbar sein. Willst du die Schablone zusammenrollen oder knicken können, benutze als Material eine Wachstuchtischdecke und einen elastischen Kleber.

12.5.1 Was wird benötigt?

- ein aussagekräftiges Motiv
- Fußbodenbelag (Linoleum) oder Pappe (Dicke 2 - 3 mm) oder eine Wachstuchtischdecke in ausreichender Größe
- Teppichmesser
- Schere
- Reiszwecken

Falls die Schablone nach dem Ausschneiden instabil ist, sodass sie sich nicht einfach an die Wand bringen lässt, muss die Schablone stabilisiert werden.
Dazu brauchst du:

- 1 Fliegengitter (oder ähnliches Netz welches nicht zu dick ist!)
- Heißklebepistole oder elastischen Kleber
- ab einer Größe von ca. 70cm x 70cm sollte die Schablone durch einen Holzrahmen stabilisiert werden

Wenn das Motiv bereits in digitaler Form vorliegt, muss es mit einem Grafikprogramm so bearbeitet werden, dass es nur noch aus Konturen oder einer Farbe besteht. Wichtig dabei ist, dass das Motiv immer noch gut zu erkennen ist

Hier ein allgemeiner Ablauf für das Bearbeites des Bildes mit Gimp (kostenfrei im Netz herunterladen - Suche: download Gimp) oder Photoshop:

- Bild „weichzeichnen“ mittels Gauschen Weichzeichner

- auf schwarz/weiß-Modus ändern
- mit Autokontrast verbessern
- Bild auf 5 Farben reduzieren. Stichwort: Tontrennung, posterisieren
- Kontrast ein wenig verringern und Helligkeit wenig erhöhen
- Bild auf 2 Farben reduzieren (wie oben)

12.5.2 Motiv zeichnen und ausschneiden

Du hast einen Polylux/Overheadprojektor:
Du druckst das Motiv auf einer Folie aus und bringst den Fußbodenbelag an eine Wand an. Nun projizierst du das Motiv auf den Belag. Mit einen wasserfesten Stift zeichnest du das Motiv nach. (Achte bei Pappe auf deinen Untergrund.) Danach nimmst du das Teppichmesser und schneidest das Motiv aus. Der Polylux/Overheadprojektor muss im Winkel von 90 Grad zu der Wand stehen, damit keine Verzerrungen entstehen, es sein denn dies ist erwünscht

Du hast keinen Polylux/Overheadprojektor:
Du solltest dich gut mit deinem Grafikprogramm auskennen! Messe aus, wie groß das Motiv werden soll. Dann rechne aus, auf wie viel A4-Blätter das Motiv passt. Nun teile mit Hilfslinien das Motiv so auf, dass es auf die vorher errechnete Anzahl von Blättern passt. Mit dem Auswahlrahmen ziehst du jedes Blatt nach, kopieren es, und fügst jedes in ein neues Bild ein. Speichere alle einzelnen Bilder ab und drucke diese aus. Wenn du sauber gearbeitet hast, kannst du nachdem du den Druckrand mit der Schere abgeschnitten hast, die einzelnen Blätter wie ein Puzzle zusammenlegen. Mit den Reiszwecken kannst du nun die Blätter auf dem Belag befestigen und das Motiv mit einen wasserfesten Stift nachzeichnen. Mit dem Teppichmesser wird das Motiv ausgeschnitten. Achte auf Sauberkeit und darauf, dass der Untergrund nicht beschädigt wird.

12.5.3 Falls die Schablone instabil ist

Wenn die Schablone nun ziemlich instabil ist und sich das Motiv noch nicht in den perfekten Formen zeigt, musst du sie stabilisieren. Dies gelingt mit einem Fliegengitter. Bringe dazu testweise Heißkleber auf beide Seiten der Schablone auf und lasse ihn abhärten. Indem du die Klebestücke wieder abreißt, testest du auf welcher Seite der Kleber am besten hält. Dort klebst du dann das Fliegengitter auf.

Anschließend legst du die Schablone in ihre spätere Form. Danach kommt das Fliegengitter drauf. Mit einer Kreisbewegung schmierst du in Größe einer Zwei-Euro-Münze flach den Kleber auf die oberste rechte Ecke des Fliegengitters. In einem Abstand von ca. 3 - 4 cm bringst du auf dem kompletten Motiv Kleber auf. Auf Schwachstellen wie Inseln oder besonders belastete Zonen muss zusätzlich Kleber aufgebracht werden. Nicht zu dicht auf den Rand schmieren. Nach dem Aushärten des Klebers, kann das Motiv testweise aufgerichtet werden.

Sollte jetzt noch irgendwas nicht sitzen wie es soll, muss mit Kleber nachgeholfen werden. Achte dabei darauf, dass die Schablone stabil sein muss, damit es später keine bösen Überraschungen gibt! Nachdem du mit Heißkleber gearbeitet hast, kannst du die Schablone nicht mehr zusammenrollen oder knicken, da sich sonst der Kleber wieder lößt.

12.5.4 Kreative Anwandlung

Solltest du mitten in der Nacht aufwachen und das Bedürfnis haben deine Garage zu verschönern, dann schüttele die Dosen ca. 15 Minuten bei dir zu Hause gut durch, damit du deine Nachbarn nicht aus dem Schlaf holst. Ein starker Magnet an der Unterseite der Dose verhindert zusätzliches

unnötiges klappern. Prüfe auch die Funktion der Dosen! Sprühe nur mit Einweghandschuhen damit du nicht noch eine Woche später mit bunten Fingern rumläufst.

Die Schablone sowie die Handschuhe solltest du, nachdem dein Kunstwerk fertiggestellt ist verbrennen, da dir der Farbgeruch zu Hause nur Kopfschmerzen bereiten würde. Bedenke, dass du die Dose nicht einfach bei dir in den Müll wirfst. (Das ist nicht nur eine Frage des Umweltschutzes.)

12.6 Wie erstellt man einen Spuckie?

Spuckies sind kleine Aufkleber, die im Gegensatz zu richtigen Stickern nicht mit einer selbstklebenden Fläche versehen sind, sondern ähnlich wie Briefmarken einseitig vorgummierte Klebeflächen haben. Diese werden zum Beispiel durch Anlecken befeuchtet und können dann auf möglichst saubere und glatte Flächen geklebt werden.

Spuckies finden oft Verwendung als Medium für politische Botschaften, sind in der Bewegung beliebt und als günstige Alternative zu Stickern sehr etabliert. Die Vorteile von Spuckies gegenüber „normalen“ Aufklebern sind eindeutig der Preis und die sehr einfache Herstellungsart. Alle die einen Drucker, ein kleines Grafik-/Schriftprogramm und einen Copyshop in der Nähe haben, sind in der Lage für wenig Geld Spuckies in großer Menge herzustellen. Nachteilig ist jedoch die kurze Lebensdauer. Da Spuckies auf einfachem Papier gedruckt werden, halten sie Wind und Wetter nicht so lange stand wie „richtige“ Aufkleber und verblassen bereits nach wenigen Wochen.

12.6.1 Was wird benötigt?

Es braucht nicht viel um leicht Spuckies herstellen zu können.

Eine Vorlage oder einen Computer zum Erstellen der Vorlage
Heimdrucker oder besser Copyshop
Einseitig vorgummiertes Papier
Schere oder besser eine Papierschneidemaschine

12.6.2 Wo kriegst du einseitig vorgummiertes Papier her?

Das Papier bekommst du entweder in einem Copyshop, Bastelladen oder im Weltnetz. Es kann unter Umständen etwas Zeit in Anspruch nehmen eine Bezugsquelle zu finden.

Copyshop
Hier solltest du Recht gute Chancen haben zu bekommen was du suchst und dass meist auch zu einem günstigen Preis. Zudem kannst du dein Papier auch gleich bedrucken lassen. Aber dazu später mehr. Je größer der Copyshop, desto größer ist deine Erfolgschance.

Bastelladen
Meist die etwas teure Alternative zum Copyshop, aber mit etwas Suchaufwand solltest du auch hier fündig werden. Auch hier gilt, je größer der Bastelladen, desto größer ist deine Erfolgschance.

Weltnetz
Lohnt sich durch die Versandkosten meist nur bei größeren Bestellmengen. Aber wenn du nach trockengummiertem Papier, gummiertem Papier, vorgummiertem Papier, Etikettenpapier oder Briefmarkenpapier suchst, solltest du auch hier fündig werden.

12.6.3 Erstellen der Vorlage

Die Vorlage ist eine DIN-A4-Seite groß und voll mit den Motiven die du später verkleben willst. Es empfiehlt sich möglichst wenig weiße Fläche zwischen den einzelnen Motiven zu lassen, um Platz

und damit Papier zu sparen. Die Auflösung sollte mindestens 150 Pixel pro Zoll (dpi) betragen, optimal sind 300 - 350 dpi. Diese Einstellungen kannst du in deinem Grafikprogramm festlegen. Wer sich mit Grafikprogrammen nicht auskennt, arbeitet damit, womit er am besten zurechtkommt.

Druckvorlagen können beispielsweise ebenso mit Word und anderen Textverarbeitungsprogrammen erstellt werden. Gehe nur immer sicher, dass dein Bild ausgedruckt auch schön scharf ist.

Achte auf einen kleinen Sicherheitsabstand (1 cm) zum Rand hin! Ansonsten kann es passieren, dass Teile deines Motives nicht abgedruckt werden. Es empfiehlt sich, wenn möglich, die Motive genau nebeneinander zu platzieren, um das Ausschneiden zu erleichtern.

12.6.4 Ausdrucken der Vorlage:

Zuerst musst du dir darüber klar werden, ob du schwarz/weiß oder farbig drucken willst. In Farbe werden die Kopierkosten etwas höher und Farben verblassen auch schneller als reines schwarz/weiß. Farbig sieht aber teilweise schöner aus und fällt den Passanten eher ins Auge. Es bleibt letztlich dir und deinem Geschmack überlassen, auch schwarz/weiß-Motive können sehr ausdrucksstark sein.

Es gibt grundsätzlich zwei Möglichkeiten, wie du die Spuckies ausdrucken kannst. Entweder du bedruckst das Papier mit deinem eigenen Drucker oder du lässt es im Copyshop machen.

Der eigene Drucker
Natürlich kannst du auch deinen eigenen Drucker benutzen um die Vorlage aufs Papier zu bringen.

Druckerpatronen für Heimdrucker sind alles andere als kostengünstig
Die Druckqualität ist im Vergleich zum Copyshop schlechter
Du bist relativ anonym, was immer ein sehr großer Vorteil ist (empfohlen)

Der Copyshop[7]

Es ist günstiger als Zuhause zu drucken
Die Druckqualität ist erheblich besser
Der Zeitaufwand ist geringer
speichert die Daten und ist damit überwachbar (nicht empfohlen)

Frage nach einem Digitaldruck! Bei herkömmlichen Druckverfahren werden die Druckrollen zu heiß und die Vorgummierung schmilzt!

12.6.5 Das Ausschneiden der Spuckies

Wenn alles ausgedruckt und kopiert ist bleibt noch die harte Arbeit: das Ausschneiden.

Du kannst es natürlich mit einer Schere probieren, besser wäre jedoch eine Papierschneidemaschine wie sie in jedem Copyshop zu finden sein sollte. Damit arbeitest du schneller und sauberer.

Fertig sind deine Spuckies! Zum Anbringen einfach die gummierte Seite anlecken und verkleben. (Beachte dabei, dass dann deine DNA am Aufkleber ist. Also mit dieser Methode nichts strafbares verleben.)

[7] denkt aber daran, dass Copyshops die kopierten Materialien speichern und damit überwacht sind, für den Fall, fall ihr etwas halblegales drucken wollt

12.7 Wie erstellt man Wurfschnipsel

Wurfschnipsel sind eine sehr effektive Methode um schnell eine spontane Aktion abzuwickeln. Ob im lokalen Einkaufszentrum wenn Hochbetrieb ist oder auf dem Marktplatz nebenan. Wenn plötzlich hunderte oder gar tausende Schnipsel mit kreativem Inhalt durch die Gegend flattern, sorgt das immer für Aufmerksamkeit

12.7.1 Was wird benötigt?

Es braucht nicht viel um leicht Wurfschnipsel herstellen zu können.

Eine Vorlage oder einen Computer zum Erstellen der Vorlage
Heimdrucker (besser) oder Copyshop
Schere oder besser eine Papierschneidemaschine

12.7.2 Erstellen des Wurfschnipsels

Wie auch beim Flugblatt sollte der Inhalt genau überlegt sein, wenn du selber Schnipsel erstellen willst. Kreative und kurze Sätze bringen mehr als viele kleine Buchstaben mit viel trockenem Inhalt. Auch Grafiken sind erlaubt. Natürlich immer mit einer Weltnetzseite zur Werbung bestücken, da sonst der Verweis und somit der Sinn fehlen würde

Hilfsmittel sind hier nur Papierschneider. Es gibt manche Papierschneidemaschinen bereits ab etwa 20 Euro. Sie erleichtern die Arbeit aber enorm und sind zudem noch genauer als die alte Papierschere aus der Grundschulzeit ...

12.7.3 Nach der Aktion

Auch so etwas sorgt für Ärger - Nicht nur bei den Putzfrauen ... Es kann als Sachbeschädigung geahndet werden. Daher lieber wieder schnell verschwinden, möglichst ohne in die Kamera zu grinsen.

Viel Spaß, aber denkt dran: Nicht erwischen lassen!

12.8 Wie erstellt man eine sichere Weltnetzseite?

Wenn du eine Weltnetzseite betreiben willst aber nicht möchtest, dass jemand weiss, dass es deine Seite ist, ja dann muss eine gewisse Anonymität gewährleistet sein. Dafür gibt es Anbieter die Server im Ausland betreiben und deine persönlichen Daten verbergen oder gar nicht erst abfragen.

Warum es sowas gibt fragst du dich?

Willst du z.B. frei, ohne Zensur deine Meinung sagen können oder der Arbeitgeber oder Partner soll davon nichts erfahren. Wenn du z.B. eine Kameradschafts- oder Veranstaltungsseite erstellen würdest bekämst du eventuell Probleme mit einer Behörde. Oder willst du dich vielleicht vor teuren Abmahnungen schützen weil du deine Weltnetzseite nicht ständig auf die neuesten Vorschriften und Gesetze anpassen kannst oder willst.

Falls du so eine anonyme Seite einrichten willst musst du darauf achten, dass die Inhalte anonym dahin übertragen werden und das du die dafür anfallenden Kosten möglichst nicht über dein reguläres und offizielles Bankkonto überweist. Es sollte nichts mit dir in Zusammenhang gebracht werden können.

Achte darauf mit welchem Computer und Weltnetzzugang du das alles bewerkstelligst. Eine Lücke kann dich verraten und je nach Brisanz des Inhalts wird man sich bemühen diese Lücke auch zu

finden.

12.8.1 Anonyme Weltnetzseite, Webserver, Domains und Hosting

Einrichtung und Wartung eines anonymen Servers um darauf eine anonyme Weltnetzseite abzulegen. Ziel ist es dabei, dass weder der Server-Anbieter, noch irgendein Provider, noch eine Bank oder Kreditkartenfirma oder irgend jemand anderes herausfinden kann, von wem der Server betrieben bzw. gewartet wird.

So bist du relativ sicher vor Abmahnungen, Unterlassungserklärungen, Zensur, politischer Verfolgung usw.

Je nach Inhalt ist ein Hoster im Ausland empfehlenswert. Kostenlos und nicht unbedingt anonym, dafür meistens mit Werbeeinblendung, geht das mit Subdomains bei verschiedenen Anbietern. (Anonym registrieren) Wer hier jedoch über die Stränge schlägt wird schnell gesperrt. Also Gesetzeslage des Landes & AGB studieren und sich daran halten.

Hier ein Blog-Anbieter:

www.logr.org - (Nationales Projekt) Er ist kostenfrei und man kann sich mit einer anonymen E-Postadresse auch über Tor anmelden. Sollte dies nicht funktionieren, einfach bei Tor einen neuen Kanal für diese Seite auswählen. Diese Seite wird ausdrücklich empfohlen.
Es gibt auch professionelle und somit kostenpflichtige Angebote mit eigener Domain und Webspace. Bei der Wahl des Server-Anbieters sollte man darauf achten, dass dieser:

whois-Einträge der Domain anonymisiert oder ersetzt
keine Voratsdatenspeicherung durchführt
keine Auskünfte will (anonymes hosting)
anonymes Bezahlen möglich ist

Der Hoster sollte NIE juristisch für die Verwaltung der Domains zuständig sein. Immer trennen.

Anbieter für anonyme Domains, anonymes Hosting aus unserer politischen Bewegung sind:

www.nw.am - (Anonyme Domain - Nationales Projekt)
www.1st-amendment.info - (Nationales Webhosting Projekt)
www.ano-host.co.in - (Nationales Webhosting Projekt)

Empfohlene Anbieter für anonyme Domains, anonymes Hosting oder beides sind:

santrex.net
2x4.ru

Eine Liste mit weitern anonymen Anbietern sowie deren Eckdaten wie Besonderheiten, Serverstandorte und Zahlungsweg findest du HIER Sowohl beim Bestellvorgang, wie auch bei der Wartung und der Pflege (Datenübertragung) sollte man immer einen öffentlichen Zugang bzw. Anonymisierungsdienst verwenden. Zurückgreifen solltest du auf das Tor Netzwerk oder eine VPN-Verbindung. Natürlich kann das ganze auch kombiniert werden. Also niemals direkt auf den Server zugreifen, weder pingen (test ob er noch lebt) noch ansurfen oder was auch immer.

12.8.2 Gefahren und Sperren von Domain und oder Webserver

Ein Webauftritt (die Weltnetzseite) besteht aus mehreren Einzelteilen. Die Domain als Adresse die über einen DNS-Eintrag zum Inhalt (Webserver) führt.

Wichtig bei anonymem Webspace und Domains ist auf die anonyme Bezahlbarkeit zu achten (Paypal, Moneybookers etc. sind nicht anonym). Der Firmenstandort und Serverstandort möglichst Offshore wählen um bei juristischen Problemen ein ëinknickender Firma zu verhindern.

Im einfachsten Fall hat man Domain und Webserver beim gleichen Anbieter. Ist alles bei einem Anbieter, hat es jemand der die Seite sperren lassen möchte leicht und du hast gleich zwei Probleme, denn Domain und Webserver könnten aus vielen Gründen gesperrt werden. Es benötigt meist viel Schreibarbeit und womöglich werden sogar Strafzahlungen verlangt um die Sperren wieder rückgängig zu machen. Domain und Webspace (Webserver) sollten also besser getrennt verwaltet sein.

Bei den Domains ist folgendes zu beachten: Fast jedes Land (Staat) hat eine Domainendung, (Top Level Domain) tld genannt.
Deutschland = .de
Schweiz = .ch
USA = .us
usw.

Jedes Land bzw. die Verwaltungsstelle hat andere Gesetze & Vorschriften bei der Vergabe bzw. Sperrung ihrer Domains. Je nach tld ist man dementsprechend mehr oder weniger abschaltsicher / sperrsicher. Es kommt also immer auf den Inhalt und die Gesetzeslage an. Prüfe deshalb vor der Wahl einer Domain wie die Gesetzeslage sich mit deinem Inhalt verträgt.

Eine kurze Liste der als realtiv sicher angesehenen Domains. (Stand 08.2012) Die in Klammern sind JoinVentures mit US Firmen, also ggf. auch Problematisch.

.so
.li
.gs
.to
.ph
.tw
(.mx)
(.me)
.asia
.vn

Jeder kennt die Kino Seiten im Weltnetz. Fast alle setzen auf eine .to tld und das aus gutem Grund. Tonga, dessen tld .to ist, erlaubt es den Nutzer eine Domain vollkommen anonym zu kaufen. Leider ist eine .to Domain aber auch recht teuer.

Manche Domains (tld) können von Haus aus anonym registriert werden, bzw. der Registrar trägt irgendeine Adresse ein. **Als Domaineigentümer solltest nicht du eingetragen sein (whois-Schutz).**

Die „Internet Corporation for Assigned Names and Numbers“ (ICANN), ist für die Kernressourcen des Internet (Domain Namen, Internet Adressen, Protokolle und den Root Server) zuständig. Die ICANN ist in der Lage fast alle tld abzuschalten. Einzige Ausnahme scheint die .to (Tonga) Domain zu sein.

Wenn du eine für deine Zwecke abmahnsichere und anonyme Domain registriert hast, kannst du diese auf einen beliebigen Webserver (Inhalt, Content) zeigen lassen. Je nach dem kann es sinnvoll sein auch noch Domains in Reserve zu haben. Dies geht mit einem DNS-Eintrag beim Domainregistrar. (Dieser sollte das unterstützen) Deshalb sollte man zensurfreie DNS-Server nutzen.

Auf dem Webserver / Webspace auf einem Weltnetz-Server liegen die Inhalte (Content), die dann jeder zu sehen bekommt. Hier gibt es gleich mehrere mögliche Gründe der Sperrung. Je nach Qualität des Hostingpaketes (Webspace) hast du mehr oder weniger Anspruch auf Serverleistung die du dir mit anderen Kunden teilen musst. Wenn du den Server überlastest bleibt der Server stehen und alle Kunden auf dem Server haben ein Problem. Dein Provider wird dich also deshalb sperren oder verlangen das du etwas hochwertigeres bezahlst.

So eine Serverüberlastung kann auch von Aussen ohne dein zutun kommen, z.b. wenn jemand der etwas gegen dich hat millionen Anfragen an deine Weltnetzseite sendet. So ein Angriff von Aussen nennt sich DDoS-Attacke. Eine DDoS-Attacke ist leider in vielen Fällen sehr gut geeignet um eine Weltnetzseite lahm zu legen.

Man kann auch Webspace und Webserver mit DDoS-Protection buchen. Da werden dann die vielen Serveranfragen mehr oder weniger gut gefiltert und deine Seite wird weniger überlastet. DDoS-Protection kostet aber meist etwas extra.

Wer sich an deinem Inhalt stört kann aber auch deinem Provider eine Abmahnung (Abuse) schicken und behaupten du würdest gegen dieses oder jenes verstossen. Inwieweit dein Provider dieses dann vor einer Sperrung prüft und auch prüfen kann... ? Wenn der Provider eine eigene Rechtsabteilung hat und den Aufwand der Prüfung betreibt wirst du nicht einfach so gesperrt. Hier ist auch der Firmensitz (Gesetzeslage) des Providers und der Standort des Servers maßgeblich. All das um den Kunden zu schützen ist aufwendig und dementsprechen teuer. So kommen die oft hohen Preise zustande.

Nicht jedes Land ist für jeden Content geeignet. So ist z.B. Russland kein geeigneter Standort für Freedom of Speech oder Whistleblowing Seiten, aber für andere Seiten aus dem Grauzonenbereich (Warez) sehr gut geeignet. Spreche am besten den Inhalt deiner Seite zuvor mit dem Hoster ab!

Wie auch immer. Falls dich dein Webspace oder der gemietete Server im Stich lässt, kannst du einfach den DNS-Eintrag für Domain(s) ändern und auf einen anderen Server verknüpfen. Innerhalb von 24 h sollte dann der Inhalt wieder angezeigt werden können. Bei sensiblen Inhalten empfiehlt es sich also einen weiteren oder sogar mehrere Webserver (in verschiedenen Ländern) sowie verschiedene Domains in Reserve zu haben. Wenn Domainregistrar und Server-Provider irgendwo in Timbuktu ihren Firmensitz haben und der Server auch in einem Land steht wo Beschwerden auf taube Ohren stossen hat es der Beschwerende sehr schwer und scheut evtl. den Aufwand.

12.8.3 Domain ¡=¿ DNS ¡=¿ Webserver - Wie geht man damit um?

Wer das Ganze (Domain ¡=¿ DNS ¡=¿ Webserver) für sich kostenlos testen möchte kann folgendes tun.

- Suche dir eine kostenlose .co.cc Domain aus.
- Die Registrierung dauert 2-3 Minuten wenn du möchtest anonym mit plausiblen Phantasiedaten.
- Suche einen kostenlosen Webspaceanbieter der externe Domains (auch co.cc) zulässt.

- Nim das FREE-Paket mit der Option (Use my existing domain) und gebe deine co.cc-Domain an.
- Das geht auch anonym mit plausiblen Phantasiedaten.

Der Anbieter des Webservers teilt dir dann die Zugangsdaten mit. Mit diesen kannst du dich in der Serververwaltung einloggen.

Hier kannst du dann stöbern was man so alles damit tun kann. Irgendwo findest du auch die Angaben zum NameServer NS des Anbieters.

Meist sind es Angaben wie:

ns1.anbieter.tld & ns2.anbieter.tld

Nun gehe wieder zur Registerstelle für .co.cc Domains, logge dich ein und gehe dort zur Domainverwaltung. Dort trägst du die zwei verschiedenen Name-Server ein.

Es kann bis zu 48 Stunden dauern bis die Angaben weltweit bekannt sind und das ganze funktioniert. Du kannst natürlich auch mehrere Webserver buchen und dann die Domain auch mal auf einen anderen Webserver (Name-Server) umstellen. Auf jedem der Webserver eine andere Testseite hochladen und du wirst sehen das es funktioniert.

Nach einiger Zeit hast du genug getestet, du weisst jetzt wie es geht und hast verstanden worum es geht.

12.8.4 Kommen wir nun zu einer ernsthaften Weltnetzseite

Unsere Empfehlungen nach aktuellem Kenntnissstand sind folgende. Für einen echten Webauftritt ohne aufwändige, anstössige oder sensible Inhalte, kannst du es beim kostenlosen Testsystem belassen. Kostenlos kann allerdings diverse Nachteile haben. Zum Einarbeiten ist es ausreichend und kann dann ergänzt werden.

Die Grundlage jedes Weltnetzangebotes von der Domain abgesehen, ist der Webspace bzw. Webserver.

Webspace - Die günstigen Angebote sind Webspace mit einer Verwaltungsoberfläche. Hierbei hast du keinen direkten Zugriff auf die Grundkonfiguration des Servers. Der Server wird vom Hoster verwaltet und wird hoffentlich durch Updates auf einem sicheren Niveau gehalten. V-Server - Etwas hochwertiger sind virtuelle Server. Das sind mehrere Virtuelle Maschinen auf einem Gerät. Die VMs können vom Hoster oder von dir selbst verwaltet werden. Wenn du vollen Zugriff darauf hast, musst du dich auch selbst um die Sicherheit und Updates kümmern. Webserver - Ist ein Gerät als Hardware. Dort hast du meist Root-Rechte also vollen Zugriff. Deshalb werden die Geräte auch gerne Root-Server genannt.
Anonymes Hosting, anonyme Webserver, anonymer Webspace wo am besten buchen? Du solltest als Anfänger bzw. unerfahrener Webmaster eher bei einem deutschsprachigen Anbieter buchen. Alle diese Server stehen irgendwo in einem Rechnezentrum irgendwo auf der Welt und sind mehr oder weniger gut an das Weltnetz angebunden.

Die Angebote haben alle mehr oder weniger Leistung, Speicherplatz und weitere Zusatzleistungen. Preis-Leistung zu vergleichen ist dabei nicht so einfach. Je nach Inhalt des Angebotes sind verschiedene Zusatzleistungen wie verschlüsselte Festplatten, SSL, Backups, Support usw. wichtig.

Um sich und seine Besucher bei sensiblen Inhalten abzusichern ist folgendes wichtig.

- Sicherer Serverstandort
- Verschlüsselte Festplatten
- SSL-Verschlüsselung bei der Datenübertragung per FTP zum Server (sFTP)
- SSL-Verschlüsselung bei der Datenübertragung über den Browser (https://)
- die verwendete Software für Blogs, Forum usw. so abändern, dass sie nichts loggt oder sonst wie plaudert.
- Server-Logging deaktiviert oder nur für sehr kurze Zeit akzeptieren. (max. 24h)
- Vorhandene Server-Logs u. Anwendungs-Logs (soweit möglich) regelmässig löschen.

Standarmässig loggt jeder Webserver alle Vorgänge der Besucher und speichert dies statistisch ab. Serverlogs in falschen Händen können sehr gefährlich für den Betreiber und die Besucher werden.

Achte darauf, dass das Server-Logging deaktiviert ist oder dekativiere es selbst falls du Zugriff auf die Serverkonfiguration (Apache) hast.

Apache-Modul removeip:

sudo apt-get install libapache2-mod-removeip
sudo a2enmod removeip
/etc/init.d/apache2 force-reload
Dadurch wird anstatt der richtigen IP für jeden Clienten die IP 127.0.0.1 in die Logs geschrieben

Keine IP Adressen in die access.log schreiben:

/etc/apache2/apache2.conf
In den Zeilen, die mit „LogFormat“ beginnen, jedes „%h“ löschen, da „%h“ die IP Adresse des Clients speichert
/etc/init.d/apache2 force-reload

Gar keine access.log schreiben:

/etc/apache2/sites-available/*
(für JEDE Datei in diesem Ordner)
„CustomLog $APACHE_LOG_DIR/access.log combined“ ersetzen durch: „CustomLog /dev/null combined“
Dadurch werden die Logs nach /dev/null geschrieben, sprich gelöscht
/etc/init.d/apache2 force-reload

error.log deaktivieren:

Für die error.log gibt es keine Möglichkeit, die IP Adressen vom Logging auszuschließen.
Man muss also die kompletten Logs wieder nach /dev/null schreiben lassen:
/etc/apache2/sites-available/*
(wieder für ALLE Dateien in diesem Ordner)
/etc/apache2/apache2.conf
„ErrorLog $APACHE_LOG_DIR/error.log“ ersetzen durch: „ErrorLog /dev/null“
/etc/init.d/apache2 force-reload

Man könnte evtl. ein Script in Perl, Python oder so schreiben, dass die IP Adressen aus den error.logs löscht oder durch 127.0.0.1 ersetzt und per Cronjob ausgeführt wird.

12.8.5 Eine Weltnetzseite mit WordPress auf einem Webspace erstellen

Im Idealfall hast du deine Weltnetzseite fertig erstellt bevor du eine Domain mit dem passenden Webspace mietest. Wir gehen bei diesem Leitfaden aber erstmal vom umgekehrten Fall aus. Du hast also eine Domain und einen Webspace gemietet und nun stehst du vor der Frage wie deine Weltnetzseite aussehen sollte oder mit welchem Werkzeug du eine vernünftige Weltnetzseite erstellen könntest.

Wir greifen hier zum Teil auf einen von Dennis Giemsch verfassten Artikel im Tremonia Blog zurück, jedoch hosten wir die Seite lieber selber. Das ist zwar mit mehr Arbeit und natürlich Kosten verbunden jedoch halten wir es für die bessere Methode. Die Anleitung vom Tremonia Blog könnt ihr aber natürlich nutzen wenn ihr keinen eigenen Webspace/server habt und das WordPress auf z.B. Blogspot oder logr nutzt.

Für diesen Leitfaden benötigst du:

Bildbearbeitungssoftware z.B. Gimp (kostenfrei im Netz) für die Header-Gafik
deinen eigenen Webspace
Filezilla portable
Tor Browser Bundle WordPress CMS + Sprachpaket und Plugins

Hast du die Domain mit dem Webspace verknüpft und greifst das erste mal darauf zu (natürlich alles via Tor / VPN) wirst du eine 08/15 - Willkommens Seite sehen die auf jedem neuen Webspace hinterlegt ist. Soweit so gut, dies bedeutet zumindest das du bis hier her alles richtig gemacht hast, d.h. die Domain zeigt auf deinen Webspace.

WordPress herunterladen
Falls dies noch nicht geschehen ist startest du jetzt das Tor Browser Bundle und gehst auf **www.de.wordpress.org**. Dort lädst du dir unter dem Punkt Download die neueste Version von des WordPress CMS herunter und entpackst die heruntergeladene .zip Datei auf z.B. deinem Desktop.

Jetzt laden wir uns ein Plugin herunter das leider später per WordPress so einfach nicht gefunden werden kann. Lade dir diese Datei herunter. Der Inhalt ist ein Plugin das sich „delete_comment_ip_immediately“ nennt und auf dessen Bedeutung wir später noch zu sprechen kommen. Wenn du das .zip Archiv heruntergeladen hast öffnest du es und kopierst die Datei „delete_comment_ip_immediately.php“ in deinen WordPress Ordner unter: „wp-content“ ¿ „plugins“.

Schutz der wp-config.php
Eine der wichtigsten Datein in dem WordPress Ordner ist die „wp-config.php“. Diese darf auf gar keinen Fall, wenn sie erstmal auf deinem Webspace liegt, zugreifbar sein. Damit erst gar nicht die Chance für Hacker entstehen kann, auf diese wirklich wichtige Datei zugreifen zu können, verbieten wir jetzt per .htaccess den Zugriff von außen. Du öffnest den ganz normalen Texteditor und trägst folgendes ein:

¡files wp-config.php¿
Order deny,allow
deny from all
¡/files¿

Diese Datei speicherst du unter .htaccess ab und kopierst sie in den WordPress Ordner. .htaccess und wp-config.php müssen sich im selben Verzeichnis befinden.

cPanel

Jetzt öffnest du im Tor Browser die cPanel Seite deines Webspaces. Die Adresse und die Zugangsdaten müsstest du ja inzwischen von deinem Anbieter bekommen haben.

Hier werden wir jetzt zwei Dinge erledigen. Zum einen legen wir unter dem Punkt „FTP Accounts“ einen neuen Login mit sicherem Passwort an.

Dieser Login sollte nicht auf das Root-Verzeichnis zeigen sondern direkt auf den Ordner in dem wir die Weltnetzseite ablegen (public_html) möchten. Im Regelfall reicht es wenn du „Directory“ leer lässt. Hast du alle nötigen Daten angegeben, bestätigst du mit Create FTP Account.

Wir gehen wieder auf die Hauptseite des cPanels und suchen uns den Punkt „MySQL Databases“.

Hier legen wir jetzt einen Benutzer für MySQL und eine neue Datenbank für die WordPress Installation an. Du scrollst herunter bis du zum Punkt „MySQL User“ gelangst. Hier trägst du einen Benutzernamen und ein sicheres Passwort ein. Der Nutzername kann ruhig etwas ausgefallen sein wie z.B. dein Passwort. Es ist überhaupt nicht schlimm wenn dein Benutzername z.B. „Ha5eM4uS“ ist.

Ist das geschafft legen wir eine neue Datenbank an. Unter dem Punkt „Create a New Database“ legst du wie schon beim Benutzernamen einen etwas ausgefalleren Namen fest und bestätigst das ganze mit „Create Database“.

Nun sind wir hier auch schon fast fertig. Als letztes müssen wir die Datenbank nur noch mit dem Benutzernamen verknüpfen. Dies machst du ganz unten bei dem Punkt „Add a User to a Database“. Dort nimmst du dir den Benutzer und die Datenbank, klickst auf „ADD“ machst einen Haken bei „ALL PRIVILEGES“ und bestätigst mit „Make Changes“. Notiere dir alle erstellten Daten (Benutzername, Datenbankname und Passwort), die werden wir später wieder brauchen

Wir haben jetzt beide Punkte abgearbeitet und du kannst dich vom cPanel ausloggen und die Seite schließen.

FTP-Programm Filezilla
Als nächstes widmen wir uns dem FTP-Programm „Filezilla“. Wir empfehlen immer den Filezilla Portable herunterzuladen. Mit einem Doppelklick auf die Herunterlegadene FileZillaPortable_x.xx.x.x.paf.exe entpackst du das komplette Programm in einen von dir gewählten Ordner. Das heißt, das Programm wird nicht auf deinem Computer installiert sondern in den einen von dir gewählten Ordner und jede Aktion in Filezilla findet ausschließlich innerhalb dieses einen Ordners statt.

Wir wollen die Weltnetzseite so anonym wie möglich auf den Webspace transverieren. Dazu ist es natürlich notwendig das auch Filezilla über einen sicheren Proxy Server geleitet wird. Dazu öffnest du das FTP Programm, gehst auf ”Bearbeiten¿ „Einstellungen“ und in dem sich öffnenden Fenster auf „Generischer-Proxy“ gibst du einen Proxy Server an oder du nutzt auch hier das Tor-Netzwerk. Für das Tor-Netzwerk musst du folgende Eingaben tätigen:

Der Typ des Proxys:
SOCKS4
Der Proxy Server:
127.0.0.1
Der Host des Proxys:
9050

Damit sich Filezilla mit dem Tor-Netzwerk verbinden kann muss natürlich das Tor-Browser-Bundle bzw. der Tor-Browser im Hintergrund laufen

Hast du die Einstellungen mit „OKbeendet wird sich Filezilla über das Tor-Netzwerk mit deinem Webspace verbinden. Da wir aber nicht wollen das jemand unsere Zugangsdaten mitliest müssen wir die Verbindung zusätzlich noch verschlüsseln. Dazu gehst du auf „Datei“ ¿ „Servermanager“. Hier trägst du nach einem Klick auf Neuer Server deine Zugangsdaten bis auf das Passwort ein. Zusätzlich klickst du im Punkt „Verschlüsselungauf“ Explizites FTP über TLS erfordernund bestätigst das Ganze mit einem Klick auf „OK“.

Verbinde dich niemals unverschlüsslt mit deinem Webspace und schon gar nicht wenn sich Filezilla über das Tor-Netzwerk verbindet

Jetzt bist du soweit und kannst dich das erste mal über Filezilla mit deiner Weltnetzseite verbinden. Du klickst rechts auf den Pfeil neben dem Serversymbol und verbindest dich mit deinem eben erstellten Server oder rufst einfach wieder die Serververwaltung auf und drückst dort auf „Verbinden“.

Nach wenigen Augenblicken bist du verbunden und du hast gesehen das sich viel getan hat. In dem rechten Fenster wirst du jetzt mindestens den Ordner „cgi-bin“ sehen. Diesen Ordner kannst du löschen und nun wird der Inhalt des zuvor heruntergeladenen WordPress CMS hochgeladen. Dazu öffnest du den entpackten WordPress Ordner und ziehst den kompletten Inhalt in das Fenster. Filezilla lädt jetzt nach und nach die Dateien auf deinen Webspace, das kann ein paar Minuten dauern.

WordPress installieren
Sind alle Daten auf deinen Webspace hochgeladen kannst du diesen mit dem Tor Browser sofort öffnen und du erhälst die erste von WordPress generierte Seite. Diese informiert dich darüber welche Daten du für die Installation des CMS benötigst. Lese dir die Seite in aller Ruhe durch und bestätige mit „Los Gehts“.

Auf der nächsten Seite gibst du deine notierten MySQL Daten ein. Der „Datenbank-Server“ ist im Regelfall localhost und schon kommen wir zum „Tabellen-Präfix“. Das Tabellen-Präfix sollte auf keinen Fall auf dem Standard „wp_“ gelassen werden. Da dieser Wert nur einmalig zugewiesen wird musst du dir auch nicht merken, was du da eingibst.

Je kryptischer der Wert, desto besser, wichig ist nur das der Unterstrich am Ende erhalten bleibt. Beispiel: woprindigldanum_

Hast du alles eingegeben bestätigst du mit „Senden“ und erhälst wenn du alles richtig eingegeben hast die Nachricht das WordPress mit der Datenbank kommunizieren kann. Hier klickst du jetzt auf „Installation ausführen“.

Jetzt dauert es nicht mehr lange und du hast deine eigene WordPress Seite. Du gibst hier jetzt die geforderten Daten ein. Denke daran ein sicheres Passwort zu wählen aber noch wichtiger ist: **Wähle auch hier einen kryptischen Namen der von potenziellen Angreifern wie Antifa-Hackern nicht erraten werden kann.** Auf keinen Fall sollte der Name Admin oder Administrator heißen Mit diesem Administratoren-Konto darf auf gar keinen Fall ein Beitrag oder Kommentar geschrieben werden, da der Name unbedingt geheim gehalten werden muss. Tätige mit diesem Namen nur administrative Aktionen wie Updates o.ä.

Richte dir einen für die Beiträge usw. unter dem Reiter ”Benutzereinen neues Benutzer-Konto ein, das die Rechte-Klasse: RRedakteurbekommt.

Mit einem Klick auf „WordPress installieren“ hast du schon das Gröbste geschafft. Die Installation ist fertiggestellt und nun geht es an den Feinschliff der Weltnetzseite.

Wordpress einstellen
Bevor wir mit der Veranstaltungsseite richtig loslegen können, widmen wir uns kurz einigen allgemeinen Einstellungen. Dafür gehen wir in den Administrationsbereich (Dashboard) von WordPress und klicken im Menü auf „Einstellungen“. Dort kannst du dann unter „Einstellungen“ ¿ „Allgemein“ den Titel der Seite, die Zeitzone, die Darstellung von Zeitangaben und die Sprache einstellen. Unter „Einstellungen“ ¿„Diskussion“ kannst du dann einstellen, wie die Kommentarfunktion der Seite genutzt werden kann. Wer möchte, kann sich auch noch die restlichen Unterseiten für Einstellungen ansehen. Die meisten Einstellungen können aber so beibehalten werden.

WordPress mit Plugins absichern
Da uns schon die ganze Zeit von WordPress angezeigt wird, dass es gerne ein Plugin aktualisieren möchte, klicken wir jetzt endlich auf „Plugins“. Es gibt hunderte, wenn nicht sogar tausende Plugins für WordPress aber wir installieren jetzt nur die drei, die für unsere Sicherheit benötigt werden und der Rest fliegt raus. Diese Plugins sollten auf keiner Weltnetzseite die mit WordPress erstellt wurde fehlen

antispam-bee
delete_comment_ip_immediately
limit-login-attempts

Die erste Amtshandlung ist also? ... Wir löschen die Plugins „Akismet“ und „Hello Dolly“. Ist dies geschehen haben wir noch das von uns heruntergeladene Plugin „Delete Comment IP immediately“ vor uns. Dieses WordPress-Plugin überschreibt sofort nach der Abgabe eines Kommentars die IP-Adresse des jeweiligen Nutzers mit der IP: „0.0.0.0“. So gelangt keine Nutzer-IP in die WordPress Datenbank. Mit einem Klick auf „Aktivieren“ kannst du das Plugin jetzt einschalten.

Nun gehen wir links unter dem Reiter „Plugins“ auf „Installieren“.

Blog-Spam bekämpfen ist die Stärke von „Antispam-Bee“. Seit Jahren wird das Plugin darauf trainiert, Spam-Kommentare zuverlässig zu erkennen, blockieren und auf Wunsch auch sofort zu beseitigen. Dabei greift Antispam Bee auf unterschiedliche Techniken zu, die sich zur Identifizierung von Spam-Nachrichten bewährt haben.

Wir tippen „Antispam-Bee“ in das Suchformular oben rechts und bestätigen mit der Entertaste. Das gewünschte Plugin sollte an erster Stelle erscheinen. Wir installieren es und klicken auf der neuen Seite auf „Aktiviere dieses Plugin“.

Das Plugin „Limit Login Attempts“ bietet gleich mehrere Vorteile. Erstens reduziert es die Anzahl der möglichen Login-Versuche, zweitens ändert es die überdetaillierten Fehlermeldungen (bei nicht-erfolgreichen Loginversuchen) von WordPress ab. Standardmäßig bietet WordPress so viele Loginversuche an, wie du benötigst. Bei einem Login-Fehler zeigt es akribisch auf, ob Benutzername oder Passwort falsch waren. Limit Login Attempts ändert die Fehlermeldung dahingehend, dass nur noch Angezeigt wird, dass die Eingabe fehlerhaft war. Es wird jedoch nicht mehr deutlich, was genau der Fehler war.

Wir tippen also „Limit Login Attempts“ in das Suchformular oben rechts und bestätigen mit der Entertaste. Das gewünschte Plugin sollte an erster Stelle erscheinen. Wir installieren es und klicken auf der neuen Seite auf „Aktiviere dieses Plugin“.

WordPress anpassen
Hier muss man sagen das es „Themes“ wie Sand am Meer gibt. Sucht euch ein schönes aus und versucht euch daran. Wir übernehmen hier jetzt größtenteils den Leitfaden vom Treamonia Blog der sich mit einer Veranstaltungsseite befasst

Nachdem wir die wichtigsten Einstellungen vorgenommen haben, können wir nun unter „Design“ ¿ „Themes“ das Aussehen der Weltnetzseite festlegen. Wir wählen hier das Theme „EventPage“ aus, das speziell zur Bewerbung von Veranstaltungen erstellt wurde. Klickt dazu in der Übersicht über alle Themes auf „Anpassen“. Nun erhalten wir auf der linken Seite Felder, über die wir unsere Sonderseite mit Inhalten befüllen können.

Im Abschnitt „Header Image“ gibt es die Möglichkeit mit wenigen Klicks eine Grafik hochzuladen, die dann automatisch im Kopfbereich der Seite, sowie in verschwommener Form auch als Hintergrundgrafik eingebunden wird. Die Grafik sollte thematisch passen und mindestens 800x400px groß sein.

Unter „EventPage Optionen“ werden die wichtigsten Daten der Veranstaltung eingetragen. Dazu gehören das Motto, die Art der Veranstaltung, die Stadt, eine genaue Adresse, das Datum und die Uhrzeit. Sollte noch kein genauer Treffpunkt bekannt sein, gebt einen öffentlichen Vorabtreffpunkt (z.B. den Hauptbahnhof) an.

Der Reiter „EventPage Contactbietet die Möglichkeit eure eBrief-Adresse, eine Telefonnummer und die URL zu einer weiterführenden Weltnetzseite (z.B. die Seite eurer Aktionsgruppe) einzutragen. Die Daten werden dann unterhalb der Seite dargestellt. Außerdem erscheint, wenn ihr Kontaktdaten hinterlegt habt, in der Navigation der Menüpunkt „Kontakt“, der den Besucher nach einem Klick direkt zu den Kontaktdaten bringt.

„EventPage Social“ - Hier kannst du die URL zu einer Facebook Seite (nicht Veranstaltung), einem Twitter Benutzernamen, oder den verwendeten Hashtag für die Veranstaltung eintragen. Nutzer können dann direkt auf der Sonderseite eurer Facebook Seite oder eurem Twitter Konto folgen. Sind keine Daten für die sozialen Netzwerke hinterlegt, so werden die Buttons trotzdem angezeigt und bewerben direkt die Sonderseite.

Dann gibt es noch den Punkt „EventPage Images“. Er bietet Platz für Redner, Musikgruppen, Propagandamaterial oder Fotos. Hier kannst du bis zu sechs Fotos bzw. Grafiken hochladen und diese mit Beschriftungen versehen. Die Fotos werden dann unterhalb des Aufrufes dargestellt. Diese Bilder können z.B. zum Ankündigen der Redner, oder zum Zeigen anderer Demofotos verwenden.

Optional lässt sich sehr leicht ein Aufruf einbinden. Für die meisten Veranstaltungen gibt es einen Aufruf in Textform. Dieser Aufruf kann im Dashboard unter „Seiten“ ¿ „Erstellen“ hinterlegt und mit Bildern, Verweisen usw. aufgearbeitet werden. Anschließend kannst du unter „Design“ ¿ „Anpassen“ erneut in den Reiter „EventPage Optionen“ und dort unter „Aufruf“ die WordPress Seite auswählen, in der du den Text gespeichert hast.

Sobald der Aufruf hinterlegt wurde, wird er auf der Seite angezeigt. Außerdem haben Besucher dann auch die Möglichkeit Kommentare auf der Seite zu hinterlassen. Dazu wird in der Navigation der Punkt „Kommentare“ hinzugefügt. Wurde ein neuer Kommentar auf der Veranstaltungsseite hinzugefügt, wird der Besucher durch eine farbige Anzeige in der Navigation auf die neuen Kommentare hingewiesen. Zusätzlich gibt es die Möglichkeit, die Kommentare als RSS Feed zu abonnieren.

WordPress-Installation und Plugins immer zeitnah updaten
Mit der Veröffentlichung einer neuen WordPress-Version steigen auch die Chancen, dass ältere Versionen gehackt werden, denn mit jedem neuen Release werden die Schwachstellen beschrieben, die mit eben diesem Release behoben wurden. Auch Plugins sind immer wieder das Einfalltor für Angriffe. Deswegen achtet bitte darauf, WordPress und alle Plugins immer auf den neuesten Stand zu bringen.

12.9 Anmelden einer Demo und Umgang mit den Behörden

12.9.1 Anmeldung einer Versammlung

Das Gesetz verlangt [§ 14 VersG], dass eine Demonstration mindestens 48 Stunden vor der öffentlichen Bekanntgabe Versammlungsbehörde mitgeteilt wird. Eine Genehmigung ist allerdings nicht erforderlich. In der Regel kann die Anmeldung auch online oder per Telefon vorgenommen werden.

Es reicht meist ein Telefonat. Man sollte bei so einem Telefongespräch immer ein paar Zeugen haben (und den Rufnummernspeicher nicht löschen, wenn man einen hat), damit man nötigenfalls später nachweisen kann, dass man die Demonstration rechtzeitig bei der Polizei angemeldet hat.

§ 14 Versammlungsgesetz:

Wer die Absicht hat, eine öffentliche Versammlung unter freiem Himmel oder einen Aufzug zu veranstalten, hat dies spätestens 48 Stunden vor der Bekanntgabe der zuständigen Behörde unter Angabe des Gegenstandes der Versammlung oder des Aufzuges anzumelden.
In der Anmeldung ist anzugeben, welche Person für die Leitung der Versammlung oder des Aufzuges verantwortlich sein soll.

Angemeldet werden kann die Versammlung auch von einer juristischen Person. Die Versammlungsleitung muss jedoch von einer natürlichen Person übernommen werden.

Heißt also:

Wenn ich beispielsweise am 1. Juni 14.oo Uhr in Frankfurt demonstrieren will und wenn ich dafür nur intern aufrufe, reicht es, wenn ich das bis zum 30. Mai, 14.oo Uhr angemeldet habe. - Will ich allerdings öffentlich werben [Weltnetz, Plakate, Handzettel oder wie auch immer], muss ich 48 Stunden vor Beginn der Werbung die Demo anmelden. Wenn ich also übermorgen öffentlich Handzettel mit Einladungen verteilen will, sollte ich diese Demo heute noch anmelden; unabhängig davon, dass der Termin erst in über zwei Monaten ist.

12.9.2 Spontanversammlungen

Spontanversammlungen bzw. -demonstrationen sind Versammlungen oder Aufzüge, die nicht vorbereitet wurden, sondern aus einem aktuellen Anlass entstehen.

Hierbei wird unterschieden zwischen nicht anmeldepflichtigen Sofortversammlungen (Spontanversammlungen im engeren Sinne) und den anmeldepflichtigen Blitz- bzw. Eilversammlungen (Spontanversammlungen im weiteren Sinne).

Ein Beispiel einer ECHTEN Spontandemonstration:

Wir sitzen am Freitagabend in Dortmund in einer Kneipe und trinken gemütlich was, und dann hören wir im Radio eine Meldung: „Udo Voigt ist verhaftet worden.“ Wir sind voll empört: Eh, da schaffen die das erst nicht, diese Partei zu verbieten und sozusagen als späte Rache nehmen sie jetzt den Vorsitzenden fest?! Das kann doch nicht wahr sein, da muss man doch was gegen tun! - Also laufen wir mit dreißig Leuten aus der Kneipe heraus und skandieren: „Freiheit für Udo - sperrt Otto ein!“ Aus umliegenden Kneipen kommen noch dreißig Leute, teilweise Kameraden, teilweise Sympathisanten und teilweise Betrunkene, die es einfach gut finden, dass mal irgendwas los ist. Und während wir in Richtung des örtlichen Polizeipräsidiums marschieren, telefoniert der eine oder andere mit dem Handy noch ein paar Leute zusammen und als wir da ankommen, sind wir hundert oder mehr Leute.

In diesem Fall wäre sogar nachweisbar, dass wir eigentlich ein Bier trinken und nicht demonstrieren wollten, bis wir dann im Radio von Udo Voigts Verhaftung gehört haben und dann ging alles so schnell [sprich „spontan“], dass keiner mehr Zeit hatte, irgendwas anzumelden. So eine Aktion ist nicht anmeldeFÄHIG und daher auch nicht anmeldePFLICHTIG. Das ist völlig unabhängig von der Frage, wieviele Leute daran teilnehmen. Ob es nun zehn oder hundert sind. Natürlich, je größer die Menge ist, desto eher entsteht der Verdacht, dass es eine länger vorher geplante Aktion war. Muss aber nicht sein. Aber wenn es um ein Thema geht, das nicht nur eine kleine, politisch bewusste Minderheit betrifft, sondern wirklich eine breite Masse, dann kann es auch Spontandemonstrationen mit Tausenden von Teilnehmern geben.

12.9.3 Sofortversammlungen

Sofortversammlungen entstehen in dem Moment des aktuellen Anlasses. Der Beschluss sich zu Versammeln fällt somit zeitlich mit der tatsächlichen Versammlung zusammen. Dadurch ist in der Regel auch kein anmeldefähiger und somit auch -pflichtiger Veranstalter zu bestimmen und eine Anmeldung nicht notwendig.

12.9.4 Eilversammlungen

Um eine Blitz- bzw. Eilversammlung handelt es sich wenn die Versammlung nicht mit dem Moment des Beschlusses zur Versammlung zusammenfällt, sondern noch eine gewisse Vorbereitungszeit verbleibt, der verfolgte Zweck jedoch auch nicht mehr nach der versammlungsgesetzlich vorgegebenen Anmeldefrist von 48 Stunden erreicht werden kann.

Hier unterscheidet man sogenannte Blitz- bzw. Eildemonstrationen [„unechte Spontandemonstrationen“ und Spontandemonstrationen [„echte Spontandemonstrationen“].

Dabei bleibt die Anmeldepflicht des Veranstalters weiterhin bestehen, die Frist wird jedoch verkürzt. Notfalls kann dabei auch eine telefonische Anmeldung über den polizeilichen Notruf 110 erfolgen. Auch hier sollte man bei so einem Telefongespräch immer ein paar Zeugen haben (und den Rufnummernspeicher nicht löschen, wenn man einen hat), damit man nötigenfalls später nachweisen kann, dass man vor Beginn der Aktion die Polizei angerufen hat.

Ein Beispielsfall für eine Blitz- bzw. Eildemonstration:

Übermorgen in Hamburg kommt es zu polizeilichen Übergriffen oder sonstigem Stress und ich entschließe mich an Ort und Stelle, gleich am nächsten Tag, Sonntag, den 28. März, noch mal zu demonstrieren. Damit bin ich anmeldePFLICHTIG, weil diese Demo anmeldeFÄHIG ist. Es ist also eine „unechte Spontandemonstration“, auch wenn zwischen dem Entschluss zum Demonstrieren und der Demonstration selbst weniger als 48 Stunden liegen.

Noch ein Beispiel:

Ich habe mich nicht am Sonnabend für eine neue Demo entschlossen, sondern sitze am Sonntagmorgen mit ein paar Kameraden zusammen und einer sagt: „Eh, das von gestern sollten wir nicht durchgehen lassen; wir sind hier noch ein paar Leute und aus Hamburg und Umgebung kriegen wir auf die Schnelle auch ein paar zusammen, lasst uns doch heute Nachmittag noch eine Demo machen.“ Das entscheiden wir, sagen wir, morgens um 10.00 bei einem späten Frühstück und wollen die Demo nachmittags um 14.00 Uhr machen. AUCH DAS ist anmeldePFLICHTIG, weil anmeldeFÄHIG, denn es liegen noch vier Stunden dazwischen.